

**Partie III. LA GÉOMÉTRIE
D'UNE FORME
QUADRATIQUE, premier
épisode : LA CONIQUE**

Introduction historique

La théorie des coniques a une histoire longue et riche et il faudrait un volume entier pour l'évoquer vraiment. Je me contenterai ici de citer quelques faits parmi les plus saillants et quelques noms parmi les plus illustres.

En vérité, une bonne partie de cette histoire est déjà écrite dans l'Antiquité. Pour les Grecs, les coniques sont, comme leur nom l'indique, les sections d'un cône à base circulaire. Les historiens pensent généralement qu'il y a eu un traité d'Aristée et Euclide sur le sujet, mais on n'en a nulle trace, si bien que les deux noms essentiels que l'histoire a retenus pour la période de l'Antiquité sont ceux d'Archimède et d'Apollonius.

Archimède (-287, -212) a surtout travaillé sur les questions de mesure (aires et volumes) des coniques et des quadriques. Il montre en particulier le rapport de l'aire de l'ellipse et de son cercle directeur. L'un de ses plus beaux résultats est la fameuse quadrature du segment de parabole¹ (qui requiert d'ailleurs de nombreux résultats auxiliaires sur celle-ci, souvent prouvés par des arguments mécaniques de leviers). Il étudie aussi les sphéroïdes et conoïdes (en langage moderne, les quadriques) et calcule certains volumes limités par ceux-ci.

Apollonius (-247, -170 (?)) a laissé un traité intitulé *Des coniques* qui fait le point des résultats connus à son époque, certains plus anciens et d'autres originaux. C'est lui qui introduit le vocabulaire encore utilisé à l'heure actuelle (parabole, ellipse, hyperbole). Il étudie nombre de notions (tangentes, asymptotes, diamètres, axes, diamètres conjugués, foyers, etc.), dont certaines étaient peut-être connues avant lui. Il donne aussi, en substance, les équations de ces courbes : $y = kx^2$ pour la parabole, $xy = k$ pour l'hyperbole, $x^2/a^2 + y^2/b^2 = 1$ pour l'ellipse². On peut citer aussi un résultat qui préfigure le théorème de Bézout : *Une section de cône ne coupe pas une section de cône en plus de quatre points.*

Il ne manque pas grand chose à la théorie, sauf la définition par foyer, directrice et excentricité, qui est connue en tous cas de Pappus.

Bien que les Anciens aient déjà en leur possession l'essentiel de la théorie, les coniques vont faire l'objet d'une attention particulière jusqu'au XX-ième siècle. Il y a peu de mathématiciens dont le nom ne soit attaché, d'une manière ou d'une autre, à la théorie des coniques. Il est donc hors de question de les citer tous, mais il faut tout de même en mentionner quelques-uns. Au

¹Le mot parabole ne sera introduit que par Apollonius. Archimède parle de *section du cône droit rectangle*.

²Bien entendu, les choses ne sont pas dites ainsi. Par exemple, pour l'ellipse, il dit *Dans toute ellipse, la somme des carrés de deux diamètres conjugués quelconques est égale à la somme des carrés des axes.*

XVII-ième siècle on retiendra surtout les noms de Descartes (pour l'invention de la géométrie analytique : les coniques de ce livre, comme on le verra, seront avant tout données par des équations), de Pascal (pour son théorème sur l'hexagone inscrit), de Desargues (pour l'involution associée à un faisceau) et de Newton (pour la preuve de l'observation de Kepler³ sur les trajectoires des planètes). Le rôle de Newton ne se limite pas à la loi de la gravitation universelle. Une partie considérable de son œuvre traite directement de propriétés géométriques des coniques (notamment sur les tangentes). On en verra un petit aperçu au chapitre 3.

Au XIX-ième siècle, il faut évidemment commencer par Poncelet, inventeur des méthodes de géométrie projective qui sous-tendent ce livre, car c'est avant tout aux coniques qu'il les applique. Nous verrons à titre d'exemple, au chapitre 3, un "lemme de Poncelet" où sont utilisées deux de ses méthodes favorites : l'utilisation de la projection (ou de la transitivité) et le passage par les complexes avec le principe de continuité. Poncelet obtient de nombreux résultats nouveaux, notamment deux théorèmes sur les tangentes et surtout son fameux "porisme", que nous étudierons au chapitre 4. À côté de Poncelet, il faut se souvenir de Plücker (pour l'utilisation systématique des points cycliques), de Chasles (auteur d'un traité important sur le sujet et à qui l'on doit le calcul du nombre⁴ de coniques tangentes à cinq coniques données, sans doute le théorème le plus difficile sur les coniques), de Dandelin et Quételet (à qui l'on doit la détermination des foyers d'une section conique) et de Frégier⁵, de Cayley (qui applique aux coniques sa colossale puissance de calcul), j'en passe et de non moins illustres⁶.

Signalons, plus près de nous, qu'un grand mathématicien comme Henri Lebesgue n'a pas dédaigné d'écrire un traité sur les coniques⁷.

En ce qui concerne les formes quadratiques, elles apparaissent avec les équations des coniques (donc au XVII-ième siècle). C'est Lagrange qui, le

³Le rôle de Kepler, s'il n'est pas essentiel d'un point de vue strictement mathématique, est cependant fondamental. En effet, c'est lui qui, en découvrant que les corps célestes décrivaient des coniques, a fait passer la théorie éthérée des Grecs au statut de mathématiques appliquées, ce qui nous vaut aujourd'hui les nombreux satellites artificiels qui tournent autour de nos têtes.

⁴Il y en a 3264.

⁵Dont je ne sais pas grand chose, sinon qu'il était professeur au collège de Troyes et ancien élève de l'école polytechnique.

⁶Jacobi, Steiner, Laguerre, etc.

⁷Je ne résiste pas au plaisir de citer le début de la préface de Paul Montel : *Ce livre est le premier ouvrage posthume d'Henri Lebesgue. L'auteur s'y retrouve tout entier. Dans son attachement à la Géométrie d'abord : Lebesgue est avant tout un géomètre et sa découverte la plus éclatante, celle de l'intégrale qui porte son nom, a une origine géométrique. On ne saurait mieux dire.*

premier, établit en 1775 qu'une telle forme peut se décomposer en somme de carrés de formes linéaires (cela revient à l'existence d'une base orthogonale) et Gauss utilisera beaucoup cette méthode, notamment dans la théorie arithmétique des formes binaires ($ax^2 + bxy + cy^2$ avec a, b, c entiers). Un autre problème provient de la théorie des coniques et des quadriques : la recherche de leurs axes (dans un espace euclidien), ce qui revient à la diagonalisation des matrices symétriques. Ce problème est abordé par Euler et surtout Cauchy. Citons enfin, vers 1850, les travaux de Jacobi et Sylvester autour de l'invariance du rang et de la signature.

Le lecteur un peu géomètre regardera avec un mélange d'envie et d'effroi la place que tenaient les coniques dans les manuels jusqu'au milieu du XX-ième siècle (par exemple le livre de Deltheil et Caire [RD89b]). Il pourra peut-être se dire que cette omniprésence était un peu exagérée ; il se dira surtout que leur totale disparition dans les programmes actuels de l'enseignement secondaire ou supérieur est d'une infinie tristesse.

Chapitre 1

Rappels sur les formes quadratiques

Dans ce chapitre nous rappelons brièvement l'algèbre dont nous aurons besoin, dans cette partie et la suivante, à propos de formes quadratiques. Parmi les points abordés, signalons les notions d'orthogonalité et d'isotropie et les groupes orthogonaux.

Dans toute la partie III, on travaille sur un corps commutatif k de caractéristique différente de 2. On suppose que le lecteur a une certaine familiarité avec les notions de forme quadratique, d'orthogonalité, etc. Nous rappelons sans démonstrations les points essentiels sur le sujet, le renvoyant, par exemple, à [Per96] ou [Die70] pour des détails supplémentaires.

1.1 Formes bilinéaires et quadratiques

1.1.1 Définition. Soit E un k -espace vectoriel. On appelle **forme bilinéaire symétrique** sur E une application $\varphi : E \times E \rightarrow k$ telle que :

- 1) pour y fixé, l'application $x \mapsto \varphi(x, y)$ est linéaire,
- 2) pour tous $x, y \in E$ on a $\varphi(x, y) = \varphi(y, x)$.

Si φ est une forme bilinéaire symétrique, la **forme quadratique** associée à φ est l'application $q : E \rightarrow k$ définie par $q(x) = \varphi(x, x)$.

1.1.2 Remarque. On notera en particulier la formule, pour $x \in E$ et $\lambda \in k$: $q(\lambda x) = \lambda^2 q(x)$.

La forme quadratique q est bien déterminée par φ . Réciproquement, on a la proposition suivante (on voit apparaître ici l'une des justifications de l'hypothèse que k n'est pas de caractéristique 2) :

1.1.3 Proposition. *Si φ est une forme bilinéaire symétrique et q la forme quadratique associée, φ est bien déterminée par q grâce à la formule :*

$$\varphi(x, y) = \frac{1}{2} [q(x + y) - q(x) - q(y)].$$

On dit que φ est la **forme polaire** de q .

Nous supposons désormais que E est de dimension finie n .

Si E est muni d'une base $\mathcal{B} = (e_1, \dots, e_n)$, la forme φ est déterminée par la matrice $A \in \mathbf{M}(n, k)$ des n^2 nombres $a_{ij} = \varphi(e_i, e_j)$. En effet, si on pose $x = \sum_{i=1}^n x_i e_i$ et $y = \sum_{j=1}^n y_j e_j$ on a :

$$\varphi(x, y) = \sum_{i,j} a_{ij} x_i y_j, \quad q(x) = \sum_{i,j} a_{i,j} x_i x_j.$$

Si on convient d'appeler encore x et y les matrices colonnes des coefficients x_i, y_j , on a donc les écritures matricielles¹ de φ et q :

$$\varphi(x, y) = {}^t x A y \quad q(x) = {}^t x A x.$$

La matrice A s'appelle la matrice de φ (ou de q) relativement à la base (e_i) . C'est une matrice symétrique.

1.1.4 Exemple. Dans le cas $n = 3$, avec les coordonnées (x, y, t) , une forme quadratique $q(x, y, t)$ n'est rien d'autre qu'une fonction polynomiale homogène de degré 2 en x, y, t à coefficients dans k . Précisément, si la matrice A est

égale à $\begin{pmatrix} a & f & e \\ f & b & d \\ e & d & c \end{pmatrix}$ on a : $q(x, y, t) = ax^2 + by^2 + ct^2 + 2dyt + 2etx + 2fxy$.

La forme polaire φ est donnée par la règle de “dédoublement” :

$$\varphi((x, y, t); (x', y', t')) = axx' + byy' + ctt' + d(y't + t'y) + e(t'x + x't) + f(x'y + y'x).$$

¹En identifiant le nombre λ et la matrice dont l'unique terme est λ .

Posons, pour $y \in E$, $\varphi_y(x) = \varphi(x, y) = \varphi(y, x)$; φ_y est une forme linéaire sur E , donc un élément de E^* . La forme φ définit donc une application linéaire : $\bar{\varphi} : E \rightarrow E^*$ qui à y associe φ_y , dont la donnée équivaut à celle de φ , et dont la matrice, dans les bases (e_i) et (e_i^*) (où (e_i^*) désigne la base duale de (e_i)), n'est autre que A .

1.1.5 Définition. On dit que φ (ou q) est **non dégénérée** si l'application $\bar{\varphi}$ est injective. Comme E est de dimension finie, il revient au même de dire que $\bar{\varphi}$ est bijective. La forme φ est non dégénérée si et seulement si $\text{Ker } \bar{\varphi}$ est nul, avec

$$\text{Ker } \bar{\varphi} = \{y \in E \mid \forall x \in E, \varphi(x, y) = 0\}.$$

Par abus de langage, le sous-espace $\text{Ker } \bar{\varphi}$ s'appelle aussi le **noyau** de φ (ou de q) et le **rang** de φ (ou de q) est, par définition, celui de $\bar{\varphi}$.

Comme E est de dimension finie, φ est non dégénérée si et seulement si $\det A$ est non nul. Ce déterminant est appelé le **discriminant** de φ (ou de q) dans la base \mathcal{B} et on le note $\Delta_{\mathcal{B}}(\varphi)$ ou $\Delta_{\mathcal{B}}(q)$.

1.1.6 Remarque. On notera que si on fait un changement de base de matrice P , la nouvelle matrice de φ est $A' = {}^t P A P$ et qu'on a donc $\det A' = \delta^2 \det A$ avec $\delta = \det P \neq 0$. Le discriminant de φ n'est donc défini qu'à un carré de k^* près.

Une conséquence de cette remarque est l'identité suivante :

1.1.7 Proposition. Soit E un espace vectoriel muni d'une forme quadratique q de forme polaire φ . Soit \mathcal{B} une base de E , $\Delta_{\mathcal{B}}(q)$ le discriminant de q dans cette base, et soit a_1, a_2, \dots, a_n une famille de vecteurs de E . On a l'identité :

$$\det_{\mathcal{B}}(a_1, \dots, a_n)^2 \Delta_{\mathcal{B}}(q) = \begin{vmatrix} q(a_1) & \varphi(a_1, a_2) & \cdots & \varphi(a_1, a_n) \\ \varphi(a_1, a_2) & q(a_2) & \cdots & \varphi(a_2, a_n) \\ \vdots & \vdots & \cdots & \vdots \\ \varphi(a_1, a_n) & \varphi(a_2, a_n) & \cdots & q(a_n) \end{vmatrix}.$$

Démonstration. Si les vecteurs a_i forment une base c'est la remarque précédente, sinon le principe de prolongement des identités algébriques (voir Partie II, ??) conclut.

1.1.8 Corollaire. (Identité de Lagrange)

On suppose E de dimension 2. Soient a, b deux vecteurs écrits dans une base \mathcal{B} donnée et notons $[a, b]$ leur déterminant. On a la formule : $[a, b]^2 \Delta_{\mathcal{B}}(q) + \varphi(a, b)^2 = q(a)q(b)$.

Dans le cas de la dimension 3 on a la relation fondamentale suivante :

1.1.9 Corollaire. *On suppose E de dimension 3. Soient a, b, c trois vecteurs de E écrits dans une base \mathcal{B} et notons $[a, b, c]$ leur déterminant dans cette base. On a l'identité :*

$$\begin{aligned}\Delta_{\mathcal{B}}(q)[a, b, c]^2 &= q(a)q(b)q(c) + 2\varphi(b, c)\varphi(c, a)\varphi(a, b) \\ &\quad - q(a)\varphi(b, c)^2 - q(b)\varphi(c, a)^2 - q(c)\varphi(a, b)^2.\end{aligned}$$

1.2 Orthogonalité et isotropie

1.2.1 Définitions

Dans tout ce paragraphe, φ est une forme bilinéaire symétrique non dégénérée sur l'espace vectoriel E et q la forme quadratique associée. Les deux notions essentielles attachées à une forme quadratique sont celles d'orthogonalité et d'isotropie. Voici déjà les définitions liées à l'orthogonalité :

1.2.1 Définition.

1) Soient $x, y \in E$. On dit que x et y sont **orthogonaux** (relativement à φ ou à q) si on a $\varphi(x, y) = 0$. On écrit alors $x \perp y$. On dit que deux parties A, B de E sont orthogonales, et on note $A \perp B$, si on a :

$$\forall x \in A, \forall y \in B, x \perp y.$$

2) Soit A une partie de E . **L'orthogonal de A** est la partie A^\perp :

$$A^\perp = \{x \in E \mid \forall a \in A, a \perp x\}.$$

C'est un sous-espace vectoriel de E .

La proposition suivante résume l'essentiel des propriétés de l'orthogonalité :

1.2.2 Proposition.

- 1) L'application $A \mapsto A^\perp$ est décroissante vis-à-vis de l'inclusion.
- 2) Si E est de dimension n et si V est un sous-espace de dimension p de E , on a $\dim V^\perp = n - p$.
- 3) Soient V, W des sous-espaces de E . On a les formules suivantes :
 - i) $V^{\perp\perp} = V$,
 - ii) $(V + W)^\perp = V^\perp \cap W^\perp$,
 - iii) $(V \cap W)^\perp = V^\perp + W^\perp$.

1.2.3 Remarque. Si la forme q est non dégénérée, l'orthogonal x^\perp d'un vecteur x non nul est l'hyperplan d'équation φ_x .

Nous passons maintenant aux définitions concernant l'isotropie :

1.2.4 Définition.

- 1) Soit $x \in E$, $x \neq 0$. On dit que x est **isotrope** si on a $q(x) = 0$.
- 2) Un sous-espace $V \subset E$ est dit **isotrope** si on a $V \cap V^\perp \neq \{0\}$, c'est-à-dire s'il existe $x \in V$ tel que pour tout $y \in V$ on ait $\varphi(x, y) = 0$.
Il revient au même de dire que $\varphi|_V$ est dégénérée.
- 3) Soit V un sous-espace de E . On dit que V est **totale-ment isotrope** si on a $V \subset V^\perp$, ou encore, si φ , en restriction à V , est nulle.
- 4) On appelle **indice** de φ (ou de q) l'entier ν , maximum des dimensions des sous-espaces totalement isotropes.

1.2.5 Remarques.

- 1) Si $\dim E = n$, on a $\dim V^\perp = n - \dim V$ et donc, si V est totalement isotrope, on a $\dim V \leq n/2$. On a donc $\nu \leq n/2$.
- 2) S'il existe un vecteur isotrope $x \in E$, $x \neq 0$, le sous-espace Kx est totalement isotrope et donc l'indice ν de la forme est ≥ 1 .
- 3) Si ν est nul la forme φ est dite **anisotrope** (ou définie). La relation $q(x) = 0$ implique alors $x = 0$.
- 4) Le sous-espace V est isotrope si et seulement si V^\perp l'est. Si V est non isotrope l'espace E est somme directe : $E = V \oplus V^\perp$.
- 5) La formule $\dim V^\perp = n - \dim V$ est encore valable pour une forme dégénérée si et seulement si $V \cap \text{Ker } \varphi$ est nul. En effet, cela résulte du fait que V^\perp est l'orthogonal (au sens de la dualité) de $\overline{\varphi}(V)$.

1.2.2 Bases orthogonales

1.2.6 Définition. Soit q une forme quadratique de forme polaire φ (éventuellement dégénérée). Une base e_1, \dots, e_n de E est dite **orthogonale** pour q (ou φ) si on a :

$$\forall i, j, i \neq j \implies \varphi(e_i, e_j) = 0.$$

Dans une telle base, la matrice de φ est diagonale :

$$A = \begin{pmatrix} \gamma_1 & & & \\ & \ddots & & 0 \\ & & \ddots & \\ 0 & & & \ddots \\ & & & & \gamma_n \end{pmatrix}$$

avec $\gamma_i = \varphi(e_i, e_i)$. On a $\Delta(q) = \prod_i \gamma_i$.

On notera que la forme φ est non dégénérée si et seulement si tous les γ_i sont non nuls.

1.2.7 Proposition. *Il existe une base orthogonale pour q .*

1.2.3 Orthogonalité et homographies

1.2.8 Théorème. *Soit E un espace vectoriel de dimension $n \geq 2$ et soit q une forme quadratique non dégénérée sur E . L'application qui à un point \bar{a} de $\mathbf{P}(E)$, i.e. une droite (a) de E , associe l'hyperplan orthogonal $(a)^\perp$ vu comme un point de $\mathbf{P}(E^*)$ est une homographie, dont la réciproque associe à un hyperplan H de E la droite H^\perp de E .*

Démonstration. On considère l'application linéaire $\bar{\varphi} : E \rightarrow E^*$ qui à $a \in E$ associe la forme φ_a définie par $\varphi_a(x) = \varphi(a, x)$. L'application associée sur les espaces projectifs est une homographie. Comme le noyau de φ_a est l'hyperplan vectoriel orthogonal à (a) , l'identification de l'espace des hyperplans à l'espace projectif dual (voir Partie I, chapitre 1 ??) donne le résultat.

1.3 Groupe orthogonal

1.3.1 Définitions

1.3.1 Définition. *Soit φ une forme bilinéaire sur E , non dégénérée, et soit q la forme quadratique associée.*

*On appelle **isométries de E** (relativement à φ ou q) les automorphismes $u \in GL(E)$ qui vérifient :*

$$\forall x, y \in E, \varphi(u(x), u(y)) = \varphi(x, y).$$

*Les isométries forment un sous-groupe de $GL(E)$ appelé **groupe orthogonal** et noté $O(q)$.*

1.3.2 Remarques.

- 1) La définition des isométries s'étend de manière évidente au cas dégénéré ou au cas d'une application linéaire entre deux espaces différents et/ou munis de deux formes différentes.
- 2) Un élément u de $GL(E)$ est une isométrie si et seulement si il conserve la forme quadratique q , i.e. si on a :

$$\forall x \in E, q(u(x)) = \varphi(u(x), u(x)) = q(x) = \varphi(x, x).$$

- 3) Si φ a pour matrice A et u pour matrice U , u est une isométrie si et seulement si on a ${}^tUAU = A$.
- 4) Si u est une homothétie de rapport λ , u est une isométrie si et seulement si on a $\lambda^2 = 1$: les homothéties Id et $-\text{Id}$ sont des isométries, et ce sont les seules.
- 5) La relation matricielle donne $\det u = \pm 1$.

1.3.3 Définition. Le sous-groupe de $O(q)$ formé des isométries de déterminant 1 est distingué et s'appelle groupe **spécial orthogonal**, ou encore groupe orthogonal **positif**. Il est noté $SO(q)$ ou $O^+(q)$ et ses éléments s'appellent des **isométries positives** ou des **rotations**.

1.3.2 Un exemple d'isométries : les symétries

Dans la suite de cette section nous supposons $\dim E = n$ et toujours k de caractéristique différente de 2.

Rappelons que si un élément $u \in GL(E)$ vérifie $u^2 = \text{Id}$, il existe deux sous-espaces notés $E^+(u)$ et $E^-(u)$ (ou simplement E^+ et E^-) qui vérifient :

- 1) $E = E^+ \oplus E^-$,
- 2) $u|_{E^+} = \text{Id}_{E^+}$, $u|_{E^-} = -\text{Id}_{E^-}$.

Si on a $u^2 = \text{Id}$ et $u \neq \text{Id}$, on dit que u est une involution (ou encore une **symétrie**). Si $\dim E^- = 1$ (resp. 2) on dit que u est une **réflexion** (resp. un **renversement** ou un **demi-tour**).

La proposition suivante décrit les symétries orthogonales, c'est-à-dire celles qui sont dans $O(q)$.

1.3.4 Proposition. Soit $u \in GL(E)$ avec $u^2 = \text{Id}$, et soient E^+ et E^- les sous-espaces associés à u . Alors, u est une isométrie si et seulement si E^+ et E^- sont orthogonaux.

On a alors $E^+ = (E^-)^\perp$, $E^- = (E^+)^\perp$, de sorte que E^+ et E^- sont non isotropes.

Réciproquement, si $F \subset E$ est un sous-espace non isotrope, il existe une et une seule symétrie orthogonale u telle que $F = E^+(u)$.

1.3.5 Remarques.

- 1) Si u est une réflexion orthogonale, u est déterminée soit par son hyperplan $H = E^+(u)$, soit par sa droite $D = E^-(u)$. On la notera éventuellement $u = \tau_H$ ou τ_D ou encore τ_x si $x \in D$, $x \neq 0$. Il y a donc bijection entre les réflexions orthogonales, les hyperplans non isotropes et les droites non

isotropes. Notons que, si u est une réflexion, u est dans $O^-(q)$.

2) Si u est un renversement orthogonal, u est déterminé par son plan $P = E^-(u)$. Il y a bijection entre les renversements orthogonaux et les plans non isotropes. Si u est un renversement, u est dans $O^+(q)$.

3) Si x est non isotrope, on a, pour $y \in E$:

$$\tau_x(y) = y - 2 \frac{\varphi(x, y)}{\varphi(x, x)} x.$$

4) En dimension 3, les seules involutions de $O(q)$ sont $-\text{Id}$, les réflexions et les renversements.

1.3.3 Similitudes

1.3.6 Définition. Soit φ une forme bilinéaire sur E , non dégénérée, et soit q la forme quadratique associée.

Soient $u \in GL(E)$ et $\mu \in k^*$. On dit que u est une **similitude de multiplicateur** μ (relativement à φ ou q) si elle vérifie :

$$\forall x, y \in E, \varphi(u(x), u(y)) = \mu \varphi(x, y).$$

Les similitudes forment un sous-groupe de $GL(E)$ noté $GO(q)$.

1.3.7 Remarques.

1) Pour que u soit une similitude de multiplicateur μ il faut et il suffit que l'on ait $q(u(x)) = \mu q(x)$ pour tout $x \in E$.

2) L'application qui à une similitude u associe son multiplicateur est un homomorphisme de $GO(q)$ dans k^* dont le noyau est le groupe des isométries. Cet homomorphisme n'est pas surjectif en général comme le montre le cas de la forme euclidienne sur \mathbf{R} .

3) Une isométrie est une similitude de multiplicateur 1, une homothétie de rapport λ est une similitude de multiplicateur λ^2 . En général, le groupe $GO(q)$ n'est pas engendré par les isométries et les homothéties, voir [Per96] Ch. V, §5, Ex. 3.

1.3.4 Classification des formes quadratiques

1.3.8 Définition. Soient q, q' deux formes quadratiques sur E . On dit que q et q' sont **équivalentes** et on note $q \sim q'$ s'il existe $u \in GL(E)$ tel que l'on ait :

$$\forall x \in E, q'(x) = q(u(x)).$$

Si les matrices de q et q' dans une base de E sont A et A' , il revient au même de dire qu'il existe une matrice P inversible telle que $A' = {}^t P A P$.

1.3.9 Remarque. Si q et q' sont équivalentes, les groupes d'isométries correspondants sont conjugués dans $GL(E)$.

Le problème de la classification des formes consiste à trouver les classes d'équivalence pour la relation \sim et si possible à les caractériser par des invariants numériques. Sur un corps quelconque c'est en général un problème très difficile.

On a des **conditions nécessaires** d'équivalence. Si $q \sim q'$ on a :

- 1) $\text{rg}(q) = \text{rg}(q')$ (égalité des rangs),
- 2) $\nu(q) = \nu(q')$ (égalité des indices),
- 3) si $\Delta(q)$ est un discriminant de q dans une base quelconque, on a $\Delta(q) = \Delta(q')$ dans k^*/k^{*2} .

Mais ces conditions ne sont pas suffisantes en général (on pensera aux formes $x^2 + y^2$ et $-x^2 - y^2$ sur \mathbf{R}).

Dans le cas de \mathbf{R} on déduit facilement de l'existence des bases orthogonales le théorème suivant (voir [Per96]) :

1.3.10 Théorème. (Théorème de Sylvester) *On suppose $k = \mathbf{R}$. Toute forme quadratique q non dégénérée sur un espace vectoriel de dimension n est équivalente à l'une (et une seule) des formes suivantes, définies sur \mathbf{R}^n :*

$$q_{p,n-p}(x_1, \dots, x_n) = \sum_{i=1}^p x_i^2 - \sum_{i=p+1}^n x_i^2$$

où p est un entier vérifiant $0 \leq p \leq n$. Le couple $(p, n-p)$ est appelé la **signature** de la forme q . La forme q est anisotrope si et seulement si p est égal à 0 ou à n .

Le corollaire suivant sera précieux :

1.3.11 Corollaire. *Si F est un sous-espace non isotrope de E , de dimension d , et si la restriction $q|_F$ est de signature $(a, d-a)$, l'orthogonal F^\perp est non isotrope et de signature $(p-a, n-d-(p-a))$.*

Démonstration. On a une base orthogonale de F avec a vecteurs positifs et $d-a$ négatifs. Si la signature de q sur F^\perp est (r, s) , on a une base orthogonale de F^\perp , avec r vecteurs positifs et s négatifs. Comme on a $E = F \oplus F^\perp$, en mettant ces bases ensemble on voit que la signature de q sur E est $a + r$, $d - a + s$, d'où le résultat en vertu de l'unicité de la signature.

1.4 Dualité

Dans cette section on suppose que q est une forme quadratique **non dégénérée** et on note φ sa forme polaire.

Soit $\bar{\varphi} : E \rightarrow E^*$ l'application linéaire associée, définie par $\bar{\varphi}(y) = \varphi_y$ avec $\varphi_y(x) = \varphi(x, y)$. Dire que la forme q est non dégénérée signifie que $\bar{\varphi}$ est un isomorphisme. Comme E est de dimension finie, il est canoniquement isomorphe à son bidual E^{**} par l'application γ qui à x associe x^* définie par $x^*(f) = f(x)$. L'isomorphisme $\psi = \gamma \circ \bar{\varphi}^{-1}$ de E^* sur E^{**} définit une forme bilinéaire φ^* (et une forme quadratique q^*) sur E^* par la formule : $\varphi^*(f, g) = \psi(g)(f) = f(\bar{\varphi}^{-1}(g))$. Si on écrit f, g sous la forme $f = \varphi_x, g = \varphi_y$ avec $x, y \in E$, on a $\varphi^*(f, g) = \varphi^*(\varphi_x, \varphi_y) = \varphi_x(\bar{\varphi}^{-1}(\varphi_y)) = \varphi_x(y) = \varphi(y, x)$, ce qui montre la symétrie de φ^* . On a aussi $q^*(\varphi_x) = q(x)$.

1.4.1 Proposition. *Si la matrice de q dans la base e_1, \dots, e_n est A , celle de q^* dans la base duale e_1^*, \dots, e_n^* est A^{-1} .*

Démonstration. Comme A est aussi la matrice de $\bar{\varphi}$ dans les bases (e_i) et (e_i^*) , la matrice $A^{-1} = (b_{ij})$ est la matrice de $\bar{\varphi}^{-1}$ dans les bases (e_i^*) et (e_i) . On calcule alors $\varphi^*(e_i^*, e_j^*) = e_i^*(\bar{\varphi}^{-1}(e_j^*)) = e_i^*(\sum_{i=1}^n b_{ij} e_i) = b_{ij}$.

La proposition montre que la donnée de la forme q et celle de q^* sont équivalentes. On vérifie (par exemple matriciellement) que l'application $u \mapsto {}^t(u^{-1})$ définit un isomorphisme de $O(q)$ sur $O(q^*)$.

La proposition suivante montre que cette définition est compatible avec la notion d'isotropie :

1.4.2 Proposition. *Soit H un hyperplan de E d'équation $f \in E^*$. Alors, H est isotrope pour q si et seulement si f est isotrope pour q^* , i.e. si on a $q^*(f) = 0$.*

Démonstration. On écrit f sous la forme $f = \varphi_x$ avec $x \in E$. On a donc $H = \text{Ker } f = \text{Ker } \varphi_x = x^\perp$ et H est isotrope si et seulement si x l'est (cf. 1.2.5.4). Comme on a $q^*(f) = q(x)$, on voit que H est isotrope si et seulement si $q^*(f)$ est nul.

Chapitre 2

Les coniques du plan projectif : généralités

Dans ce chapitre et les deux suivants nous étudions les coniques projectives. Hormis quelques incursions fugaces dans le domaine de la géométrie affine, nous nous en tiendrons au cadre projectif, même si, sur ces questions, il est parfois très réducteur. Bien entendu, cette vision des coniques n'est pas du tout conforme à l'approche historique. Le lecteur, qui souhaiterait étudier les coniques euclidiennes (y compris avec des méthodes projectives) et n'aurait pas la patience d'attendre notre partie VI, ira consulter [Ber90] ou [RD89a]. Ce chapitre aborde en particulier les notions de tangente, de polaire et la classification projective des coniques.

Soit E un k -espace vectoriel¹ de dimension 3, $\mathbf{P}(E)$ le plan projectif associé et p la projection de $E - \{0\}$ sur $\mathbf{P}(E)$. On note Q l'espace vectoriel des formes quadratiques sur E . Cet espace est de dimension 6 car il est isomorphe à celui des matrices 3×3 symétriques.

2.1 Définition des coniques

2.1.1 Première définition

2.1.1 Définition. On appelle **conique** de $\mathbf{P}(E)$ un élément \bar{q} de l'espace projectif $\mathbf{P}(Q)$, i.e. une forme quadratique q non nulle, définie à un sca-

¹Le corps est toujours de caractéristique $\neq 2$.

laire près. On dit que q est une équation de la conique \bar{q} . Une conique \bar{q} est dite **propre** si la forme q est non dégénérée, impropre (ou singulière, ou dégénérée), sinon (bien entendu, cette notion ne dépend que de \bar{q} , pas de l'équation particulière q).

Si \bar{q} est une conique de $\mathbf{P}(E)$, on appelle **conique duale** la conique \bar{q}^* de $\mathbf{P}(E^*)$ (voir 1.4).

2.1.2 Remarque. Le lecteur qui trouverait, avec quelque raison, la définition précédente peu géométrique, est prié de patienter jusqu'au paragraphe suivant.

2.1.2 Points d'une conique

2.1.3 Proposition-Définition. Soit \bar{q} une conique et soit $\bar{m} \in \mathbf{P}(E)$. On dit que \bar{m} est un point de \bar{q} si on a, quels que soient les représentants q de \bar{q} et m de \bar{m} , $q(m) = 0$ (i.e. si m est un vecteur isotrope pour q). Il suffit pour cela que l'on ait cette propriété pour un représentant quelconque de \bar{m} et un représentant quelconque de \bar{q} . On note : $V(\bar{q}) = \{\bar{m} \in \mathbf{P}(E) \mid q(m) = 0\}$ et on dit encore que $V(\bar{q})$ est l'ensemble des zéros de \bar{q} . La conique \bar{q} sera dite non vide si $V(\bar{q})$ est non vide.

Démonstration. La seule chose à noter c'est que si λ et μ sont des scalaires non nuls, on a $(\mu q)(\lambda m) = \mu \lambda^2 q(m)$, cf. 1.1.2.

2.1.4 Remarques.

1) Disons, une fois pour toutes, que nous allons commettre de nombreux abus de langage et de notation, presque toujours innocents, autour des notions précédentes. En particulier, nous écrirons $q(m) = 0$, sans préciser si m est un point ou un vecteur et q une forme quadratique ou une conique puisque la nullité de cette quantité en est indépendante. De même, si φ est la forme polaire de q , nous écrirons $\varphi(a, b) = 0$, avec pour a, b des vecteurs de E ou des points de $\mathbf{P}(E)$. Nous noterons $V(q)$ au lieu de $V(\bar{q})$, ce qui est légitime puisqu'on a aussi $V(q) = V(\lambda q)$, pour $\lambda \in k^*$. Nous parlerons même parfois de la conique q en lieu et place de \bar{q} , lorsque cette confusion ne pose pas de problème.

2) Pour certains auteurs, une conique projective est l'ensemble des points $V(q)$ où la forme quadratique q s'annule, ou encore l'ensemble des points $(x, y, t) \in \mathbf{P}^2$ qui annulent un polynôme homogène de degré 2 :

$$ax^2 + by^2 + ct^2 + 2dyt + 2etx + 2fxy = 0.$$

Si cette définition est tout à fait convenable dans le cas des coniques propres non vides, comme nous le verrons, elle présente cependant plusieurs inconvénients. Le principal problème soulevé par cette définition est que, dans certains cas, l'ensemble $V(q)$ ne détermine pas la forme q , même à un scalaire près. Par exemple, si $k = \mathbf{R}$ et $q = X^2 + Y^2 + T^2$, $V(q)$ est vide, mais cela vaut pour toute forme q' anisotrope, par exemple $q' = X^2 + Y^2 + 2T^2$, qui n'est pas proportionnelle à q . Si $k = \mathbf{R}$ et $q = X^2 + Y^2$, $V(q)$ est réduit au point $(0, 0, 1)$, mais c'est vrai aussi pour $V(q')$ avec $q' = X^2 + 2Y^2$.

3) Le lecteur peut s'étonner de la place prise par des coniques qui n'en sont guère : vides ou réduites à un point. Il n'a pas tout à fait tort en ce qui concerne la présente partie où les coniques que nous étudierons sont essentiellement les coniques propres non vides. Il y a cependant deux raisons qui font qu'on ne peut les écarter totalement. D'abord, une conique qui n'a pas de point sur un corps donné en aura toujours dans une extension convenable (par exemple sur un corps algébriquement clos, par exemple sur \mathbf{C} dans le cas réel). Ensuite et surtout, le lecteur sceptique devra admettre, avec l'étude des géométries elliptique ou euclidienne dans les parties IV et VI, que les coniques vides ou réduites à un point sont importantes aussi, essentiellement au travers de la polarité qui leur est associée.

4) Le théorème des zéros de Hilbert (Nullstellensatz), que nous avons rencontré dans la Partie II ??, permet d'affirmer que, si k est algébriquement clos et si q, q' sont des formes quadratiques non nulles sur E ayant même ensemble de points $V(q) = V(q')$, alors ces formes sont proportionnelles, de sorte que la difficulté évoquée ci-dessus n'a pas lieu d'être. Nous verrons que ce théorème peut être amélioré dans le cas particulier des coniques.

2.1.5 Remarque. Si \bar{q} est une conique, comme q n'est définie qu'à un scalaire près et que la dimension est 3, on peut toujours supposer que le discriminant $\Delta(q)$ est un carré ou l'opposé d'un carré à notre convenance. En effet, si on pose $q' = \lambda q$, avec $\lambda = \Delta(q)$ (resp. $-\Delta(q)$), on a $\Delta(q') = \lambda^3 \Delta(q) = \Delta(q)^4$ (resp. $-\Delta(q)^4$). Si la conique est propre, on peut même supposer $\Delta(q) = 1$ (resp. -1) en effectuant le changement de base $e'_1 = e_1/\sqrt{\Delta(q)}$, $e'_2 = e_2$, $e'_3 = e_3$ (resp. $e'_1 = e_1/\sqrt{-\Delta(q)}$).

Dans ce qui suit nous choisirons généralement de prendre $\Delta(q) = -1$ (ce qui est le cas lorsqu'on considère une forme du type $X^2 + Y^2 - T^2$ ou $Y^2 - 2XT$). Les raisons de ce choix apparaîtront dans la partie suivante mais, de toute manière, c'est un choix assez innocent, puisqu'il n'affecte ni la conique \bar{q} ni le groupe orthogonal $O(q)$.

2.2 Classification des coniques

2.2.1 Définition

Les remarques précédentes nous ont déjà montré une première difficulté du lien entre conique, équation et ensemble de points. Le même type de difficulté se rencontre quand on cherche à “classifier” les coniques. Comme dans beaucoup de problèmes de classification, la traduction mathématique adéquate est en termes d’orbites. L’opération la plus naturelle est ici celle du groupe des homographies sur les ensembles de points, opération qui à $\Gamma = V(q)$ associe $\bar{u}(\Gamma)$, si \bar{u} est une homographie, mais on doit s’attendre à des problèmes importants lorsque $V(q)$ est trop petit (vide ou réduit à un point). Il est donc plus prudent de définir l’opération à partir de celle du groupe linéaire sur les formes quadratiques :

2.2.1 Définition. Le groupe $PGL(E)$ des homographies de $\mathbf{P}(E)$ opère sur l’ensemble $\mathbf{P}(Q)$ des coniques de la façon suivante : si \bar{u} est dans $PGL(E)$ et \bar{q} dans $\mathbf{P}(Q)$, on pose $\bar{u}.\bar{q} = \overline{q \circ u^{-1}}$. On a la formule : $V(\bar{u}.\bar{q}) = \bar{u}(V(\bar{q}))$

2.2.2 Remarque. La raison d’être de l’exposant -1 de la formule précédente est double. D’abord, cela fait que l’opération est “à gauche”, i.e. qu’elle vérifie : $(\bar{u}\bar{v}).\bar{q} = \bar{u}(\bar{v}.\bar{q})$. Ensuite, au niveau des ensembles de points, on retrouve bien la formule attendue. (Si on avait pris $q \circ u$, l’opération serait à droite et le u^{-1} apparaîtrait au niveau des points.)

La définition de la classification projective des coniques est alors naturelle :

2.2.3 Définition. On dit que deux coniques \bar{q} et \bar{q}' sont **projectivement équivalentes** si elles sont dans la même orbite pour l’action de $PGL(E)$ sur $\mathbf{P}(Q)$, c’est-à-dire s’il existe $u \in GL(E)$ et $\lambda \in k^*$ avec $q' = \lambda(q \circ u^{-1})$: les formes quadratiques q et q' sont équivalentes à un scalaire près.

Cette définition a une conséquence évidente sur les ensembles de points :

2.2.4 Proposition. Si les coniques \bar{q} et \bar{q}' sont projectivement équivalentes, il existe une homographie \bar{u} telle que $\bar{u}(V(\bar{q})) = V(\bar{q}')$.

2.2.5 Remarque. La réciproque de cette proposition est fausse en général. Les difficultés sont du même ordre que celles évoquées dans la remarque 2.1.4. Par exemple, si on a $k = \mathbf{Q}$, les formes $X^2 + Y^2 + T^2$ et $X^2 + Y^2 + 2T^2$ ne

sont pas équivalentes à un scalaire près (leurs discriminants 1 et 2 ne sont pas égaux dans $\mathbf{Q}^*/\mathbf{Q}^{*2}$), même si toutes deux correspondent à des coniques vides, donc ayant des ensembles de points échangés par homographie. Le théorème de Sylvester de classification des formes quadratiques (cf. 1.3.10) montre que cette difficulté ne se produit pas sur \mathbf{R} et moins encore sur \mathbf{C} (cf. [Per96]).

Notre objectif est maintenant de prouver le théorème 2.2.26 qui montre qu'il n'y a qu'une seule conique propre non vide à équivalence près. Nous avons besoin pour cela de quelques compléments sur les coniques impropres et les tangentes.

2.2.2 Coniques impropres

Rappelons qu'il s'agit des coniques correspondant aux formes dégénérées. Ces formes ont donc un noyau et on définit :

2.2.6 Définition. *Si \bar{q} est une conique impropre, on appelle **point double** de \bar{q} (ou de $V(q)$) tout point de $\mathbf{P}(E)$ image d'un vecteur du noyau $\text{Ker } q$.*



Figure 2.1: Les trois types de coniques impropres.

Le résultat suivant donne une classification complète des coniques impropres :

2.2.7 Proposition. *Deux coniques **impropres** \bar{q} et \bar{q}' sont projectivement équivalentes si et seulement si elles vérifient l'une des conditions suivantes :*

- 1) *les formes q, q' sont toutes deux de rang 1,*
- 2) *les formes q, q' sont toutes deux de rang 2 et les formes induites par q (resp. q') sur $E/\text{Ker } q$ (resp. $E/\text{Ker } q'$) ont même discriminant Δ dans k^*/k^{*2} .*

Dans le premier cas, la forme est équivalente à un scalaire près à la forme

$q = X^2$, et $V(q)$ est alors la droite $X = 0$. On dit que \bar{q} est une **droite double** et tous les points de $V(q)$ sont des points doubles.

Dans le second cas, la forme est équivalente à un scalaire près à $X^2 - \alpha Y^2$, avec $\alpha \in k^*$.

a) Si α est un carré dans k , q est, plus précisément, équivalente à un scalaire près à $X^2 - Y^2$ et $V(q)$ est la **réunion de deux droites** $X = \pm Y$. L'unique point double de q est le point d'intersection $(0, 0, 1)$ de ces droites.

b) Si α n'est pas un carré dans k , $V(q)$ est **réduite à un point** $(0, 0, 1)$ et ce point est un point double.

Démonstration. 1) Si q est de rang 1, son noyau est de dimension 2 et, en prenant pour base de E , une base e_1, e_2, e_3 avec $e_2, e_3 \in \text{Ker } q$ on voit que q est de la forme λX^2 et on a le résultat.

2) Si le noyau est de rang 1, on prend une base e_1, e_2, e_3 de E orthogonale pour q , avec $\text{Ker } q = (e_3)$. On a alors $q = \lambda X^2 + \mu Y^2$ avec $\lambda, \mu \neq 0$ et, à un scalaire près, on peut supposer $q = X^2 - \alpha Y^2$. Il est clair que deux telles formes q, q' , relatives à α, α' sont équivalentes si et seulement elles le sont comme formes en les seules variables X, Y , autrement dit si les formes qu'elles induisent sur $E/\text{Ker } q$ et $E/\text{Ker } q'$ le sont. Il faut pour cela que ces formes aient même discriminant dans k^*/k^{*2} , ce qui signifie qu'on a $\alpha' = \lambda^2 \alpha$, et cela suffit car on passe alors de q à q' en changeant e_2 en λe_2 .

Du point de vue de $V(q)$, il y a deux cas à distinguer :

a) Si α est un carré, $\alpha = \beta^2$, le changement de base $e'_2 = e_2/\beta$ montre que q est équivalente à $X^2 - Y^2$ et $V(q)$ est formé des deux droites $X = \pm Y$.

b) Si α n'est pas un carré, il est clair que $V(q)$ est réduite au point $(0, 0, 1)$.

2.2.8 Remarques.

1) On notera la différence entre les deux cas de rang 2 : les coniques réunions de deux droites sont toutes projectivement équivalentes, mais pas celles réduites à un point. Précisément, les formes $q = X^2 - \alpha Y^2$ et $q' = X^2 - \alpha' Y^2$ sont équivalentes si et seulement si α/α' est un carré de k . Sur \mathbf{Q} , par exemple, les formes $q = X^2 - 2Y^2$ et $q' = X^2 - 3Y^2$ ne sont donc pas équivalentes.

2) Si $V(q)$ est réunion de deux droites D_1, D_2 , on retrouve le fait que la forme q est bien déterminée à un scalaire près en prenant comme repère a, b, c, d avec $c = (0, 0, 1)$ à l'intersection des droites, $a = (1, 0, 0)$ sur D_1 , $b = (0, 1, 0)$ sur D_2 et $d \notin D_1 \cup D_2$. Dans ce repère, on a $q = \lambda XY$.

2.2.3 Intersection d'une droite et d'une conique, tangentes

Détermination de l'intersection d'une conique et d'une droite

Dans ce paragraphe nous examinons les positions possibles d'une conique et d'une droite. Soit q une conique, Γ l'ensemble des points de q et soit D une droite. On cherche l'intersection $\Gamma \cap D$. Soient a, b deux points distincts de D , de sorte que les autres points de D s'écrivent $m = \lambda a + \mu b$ avec $\lambda, \mu \in k$, non tous deux nuls. On doit résoudre l'équation $q(\lambda a + \mu b) = 0$. En développant cette expression on obtient :

$$q(\lambda a + \mu b) = \lambda^2 q(a) + 2\lambda\mu \varphi(a, b) + \mu^2 q(b) = 0.$$

Il y a deux cas :

1) Si on a $q(a) = q(b) = \varphi(a, b) = 0$, tous les points de D sont dans Γ . En termes de vecteurs isotropes, cela signifie que le plan vectoriel $F = p^{-1}(D)$ est totalement isotrope, ce qui n'est possible que si la forme q est dégénérée. On est donc dans le cas d'une conique impropre, réunion de deux droites ou droite double, avec D contenue dans Γ .

2) Si $q(a), q(b)$ et $\varphi(a, b)$ ne sont pas tous nuls, la droite n'est pas contenue dans Γ et, quitte à changer les points a et b , on peut supposer $a \notin \Gamma$, c'est-à-dire $q(a) \neq 0$. Comme a n'est pas sur Γ on peut se limiter à chercher les points m vérifiant $\mu \neq 0$ ou même $\mu = 1$ et l'équation se réduit alors à une équation du second degré en λ . On a donc $|\Gamma \cap D| \leq 2$. On dit que D est **extérieure** à Γ si $\Gamma \cap D$ est vide, qu'elle est **tangente** si $\Gamma \cap D$ contient un unique point et qu'elle est **sécante** s'il en contient 2.

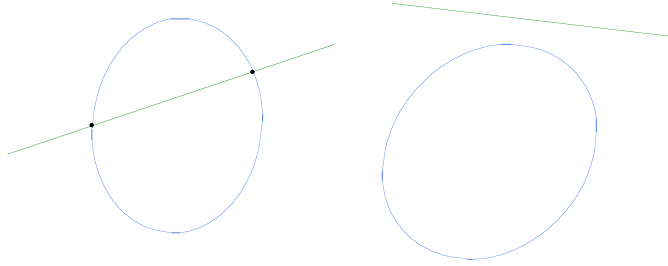


Figure 2.2: Les cas des droites sécante et extérieure.

On notera que si k est algébriquement clos, seuls les deux derniers cas peuvent se produire. Dans tous les cas on a établi l'énoncé suivant :

2.2.9 Proposition. (tout petit Bézout) Soit Γ une conique propre et D une droite. On a $|\Gamma \cap D| \leq 2$.

2.2.10 Remarque. On notera aussi que la droite D est tangente si et seulement si le discriminant de l'équation du second degré est nul. Mais, ce discriminant n'est autre que $4(\varphi(a, b)^2 - q(a)q(b))$ i.e. $4\Delta(q|_F)$ où F est le plan

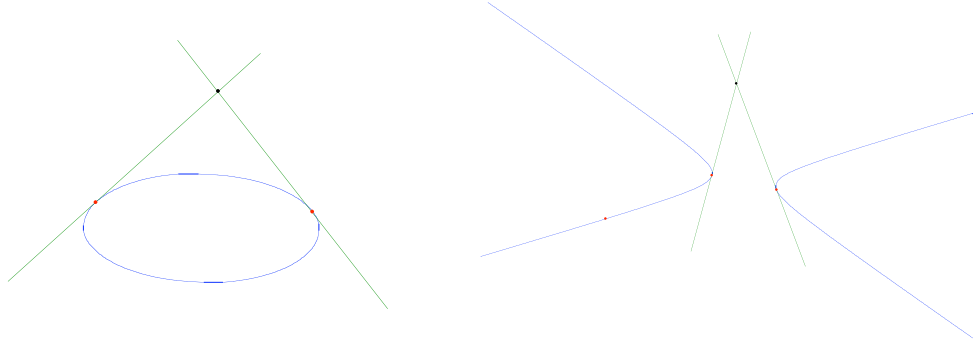


Figure 2.3: Les tangentes issues d'un point à une ellipse et une hyperbole

vectorel $p^{-1}(D)$. Le cas de tangence correspond donc au cas où ce sous-espace est isotrope pour q .

Tangentes

En fait, il est commode d'englober le cas où la droite est incluse dans la conique dans les tangentes. On propose donc la définition suivante :

2.2.11 Définition. Soit \bar{q} une conique, $\Gamma = V(\bar{q})$ et soit D une droite. On dit que D est tangente à Γ si l'une des conditions suivantes est réalisée :

- 1) $D \subset \Gamma$,
- 2) $|D \cap \Gamma| = 1$.

Cela comprend donc les cas suivants :

- 1.a) la conique est une droite double et D est la droite en question,
- 1.b) la conique est réunion de deux droites, dont D ,
- 2.a) la conique est une droite double et D une droite quelconque,
- 2.b) la conique est dégénérée réduite à un point et D passe par ce point,
- 2.c) la conique est réunion de deux droites et D passe par le point d'intersection,
- 2.d) la conique est propre non vide et $D \cap \Gamma$ contient un unique point appelé **point de contact** de D et Γ .

On notera en particulier que toute droite qui contient un point double est une tangente au sens ci-dessus.

Interprétation en termes de formes quadratiques

La définition précédente a une interprétation algébrique simple :

2.2.12 Proposition. Soit \bar{q} une conique et D une droite de $\mathbf{P}(E)$, image du plan vectoriel F . Soit a, b une base de F . Les propriétés suivantes sont équivalentes :

- 1) D est tangente à \bar{q} ,
- 2) F est isotrope pour q (i.e. $q|_F$ est dégénérée),
- 3) on a $q(a)q(b) = \varphi(a, b)^2$,
- 4) le discriminant de $q|_F$ est nul.

Démonstration. L'équivalence de 1) et 2) a été vue ci-dessus, cf. notamment 2.2.10 et les points 3) et 4) sont des traductions de 2).

2.2.13 Remarque. Rappelons que D peut être vue aussi comme un point de $\mathbf{P}(E^*)$. Si la conique \bar{q} est propre, la proposition 1.4.2 montre que D est tangente à $V(\bar{q})$ si et seulement si D est un point de la conique duale \bar{q}^* .

Dans la même veine, on peut caractériser le cas où l'intersection d'une conique et d'une droite est formée de deux points :

2.2.14 Proposition. Soit $\Gamma = \bar{q}$ une conique propre et soit D une droite, image du plan vectoriel F . L'intersection de Γ et D est formée de deux points distincts si et seulement si le discriminant de $q|_F$ est l'opposé d'un carré non nul de k .

Démonstration. Il s'agit d'exprimer que le plan F contient exactement deux droites isotropes, ce qui signifie encore qu'il est hyperbolique, ou encore que $q|_F$ est de déterminant -1 modulo les carrés (voir [Per96] Ch. VIII, Prop. 2.5 et 2.3).

Quelques problèmes sur les tangentes

Nous cherchons ici combien de tangentes à une conique propre passent par un point m_0 donné. Le premier cas est celui où m_0 est sur Γ :

2.2.15 Proposition. (Tangente en un point de Γ) Soit \bar{q} une conique propre non vide, $\Gamma = V(q)$ et soit $a \in \Gamma$. Il y a une unique droite tangente à \bar{q} passant par a . Cette droite est l'ensemble des points m qui vérifient $\varphi(a, m) = 0$. C'est l'image du sous-espace a^\perp orthogonal à a dans E (i.e., la polaire de a , voir 2.3.3).

Démonstration. Cela résulte de 2.2.12.3 puisque $q(a)$ est nul.

2.2.16 Corollaire. Soit \bar{q} une conique propre non vide, $\Gamma = V(q)$ et soit $a \in \Gamma$. À l'exception de la tangente, toute droite passant par a coupe la conique en un deuxième point.

2.2.17 Remarque. L'équation de la tangente en a à $\Gamma = V(q)$ est donc $\varphi(a, m) = 0$. Si on a $q(x, y, t) = \alpha x^2 + \beta y^2 + \gamma t^2 + 2\delta yt + 2\epsilon tx + 2\eta xy = 0$, et si on pose $m = (x, y, t)$ et $a = (u, v, w)$, cette équation s'écrit :

$$\alpha ux + \beta vy + \gamma wt + \delta(wy + vt) + \epsilon(ut + wx) + \eta(vx + uy) = 0.$$

2.2.18 Proposition. Soit \bar{q} une conique propre non vide, $\Gamma = V(q)$ et soit $a \in \mathbf{P}(E)$, $a \notin \Gamma$. Il y a 0 ou 2 droites tangentes à Γ passant par a . Les points de contact des tangentes sont les points d'intersection de Γ et de la droite d'équation $\varphi(a, m) = 0$ (la polaire de a , voir 2.3.3).

Démonstration. Soit $m \in \Gamma$. En vertu de 2.2.12.3, dire que la droite (ma) est tangente signifie qu'on a $\varphi(a, m)^2 - q(m)q(a) = 0$, donc $\varphi(a, m) = 0$. L'ensemble des points m de $\mathbf{P}(E)$ vérifiant $\varphi(a, m) = 0$ est l'image du sous-espace a^\perp orthogonal à a (a étant vu comme une droite de E). Comme q est non dégénérée, ce sous-espace est un plan, donc son image, notée encore a^\perp , est une droite. Il y a au plus deux points d'intersection entre a^\perp et Γ en vertu de 2.2.9. De plus, s'il y avait un seul point d'intersection b , la droite a^\perp serait la tangente en b à Γ . Or, on a vu à la proposition précédente qu'on aurait alors $a^\perp = b^\perp$, donc $a = (a^\perp)^\perp = (b^\perp)^\perp = b$, contrairement à l'hypothèse $a \notin \Gamma$.

Dans le cas où le corps k est le corps des réels on peut préciser ce résultat² :

2.2.19 Proposition. On suppose que k est le corps des réels. Soit \bar{q} une conique propre non vide, $\Gamma = V(q)$. On suppose que $\Delta(q)$ est égal à -1 (cf. 2.1.5).

- 1) Le complémentaire de Γ dans $\mathbf{P}(E)$ comporte deux composantes connexes \mathbf{K} et \mathbf{T} définies respectivement par $q(m) < 0$ et $q(m) > 0$ appelées respectivement intérieur et extérieur de Γ .
- 2) La partie \mathbf{T} contient des droites tandis que \mathbf{K} n'en contient pas.
- 3) Les tangentes à Γ sont toutes entières dans \mathbf{T} , à l'exception de leur point de contact. Il y a 0 (resp. 2) droites tangentes à Γ passant par $a \in \mathbf{P}(E) - \Gamma$ si a est dans \mathbf{K} (resp. dans \mathbf{T}).

Démonstration. Vu les hypothèses, le théorème de Sylvester (cf. 1.3.10) montre que q est équivalente à $X^2 + Y^2 - T^2$. On munit $\mathbf{P}(E)$ de sa topologie naturelle (voir Partie I, Ch. 1, Exercice ??). Comme q est continue sur E , son signe est une fonction continue sur $\mathbf{P}(E) - \Gamma$, ce qui montre que \mathbf{K} et \mathbf{T} en

²On retrouvera les notations de la proposition suivante dans la partie IV, en particulier la partie \mathbf{K} qui constitue le modèle de Klein du plan hyperbolique.

sont des parties ouvertes et fermées. Si l'on choisit $T = 0$ comme droite à l'infini, on voit que \mathbf{K} est tout entière dans le plan affine $T \neq 0$ et qu'elle est homéomorphe au disque unité ouvert de $\mathbf{R}^2 : x^2 + y^2 < 1$, donc connexe. Comme les droites projectives sont homéomorphes à des cercles, la connexité de \mathbf{T} résulte des deux faits suivants :

- a) la droite D_∞ est contenue dans \mathbf{T} ,
- b) par tout point m de \mathbf{T} passe une droite qui ne rencontre pas \mathbf{K} et qui coupe D_∞ . En effet, si $m = (x, y, 1)$ la droite d'équation $x(X - xT) + y(Y - yT)$ convient comme on le voit en utilisant l'inégalité de Cauchy-Schwarz :

$$|xX + yY| \leq \sqrt{x^2 + y^2} \sqrt{X^2 + Y^2}.$$

Le point 2) est évident (si \mathbf{K} contenait une droite projective, la forme serait définie négative en restriction au plan vectoriel correspondant et cela contredirait 1.3.11).

Soit \bar{a} un point de $\mathbf{P}(E) - \Gamma$. Le nombre de tangentes issues de \bar{a} est le nombre de points d'intersection de \bar{a}^\perp avec Γ , ou encore le nombre de droites isotropes de a^\perp . Si \bar{a} est dans \mathbf{T} , on a $q(a) > 0$, donc, par 1.3.11, a^\perp est un plan hyperbolique (c'est-à-dire de signature $(1, 1)$) et il y a deux droites isotropes dans a^\perp , donc deux tangentes issues de \bar{a} . Si au contraire, \bar{a} est dans \mathbf{K} , le plan a^\perp est défini positif, donc anisotrope, et \bar{a} n'est sur aucune tangente.

Il reste à montrer que si D est la tangente en $a \in \Gamma$, elle est contenue dans \mathbf{T} (à l'exception du point a). Soit m un point de D , qui vérifie donc $\varphi(a, m) = 0$. Si m est dans \mathbf{K} on a $q(m) < 0$, le point m est non isotrope et son orthogonal m^\perp est de signature $(2, 0)$, toujours en vertu de 1.3.11. Il ne contient donc pas de vecteur isotrope, ce qui contredit $\varphi(a, m) = 0$.

2.2.20 Remarque. Pour une construction géométrique de la tangente en un point $a \in \Gamma$ ou des tangentes issues d'un point $a \notin \Gamma$, voir 2.3.12 et 3.1.10.

Conique duale, conique tangentielle

Dans ce paragraphe on voit les coniques comme “enveloppes” de leurs tangentes. Le résultat est le suivant :

2.2.21 Proposition. *Soit \bar{q} une conique propre non vide, $\Gamma = V(q)$ et soit \bar{q}^* la conique duale (qui est une conique de $\mathbf{P}(E^*)$, voir 2.1.1). L'ensemble Γ^* des points de \bar{q}^* est l'ensemble des droites de $\mathbf{P}(E)$ tangentes à Γ . On dit que Γ est l'enveloppe de ses tangentes.*

Démonstration. C'est exactement 1.4.2.

2.2.22 Remarque. Le résultat précédent fait qu'on désignera parfois la conique duale comme la **conique tangentielle** associée à q . Dans la pratique, si A est la matrice de q , on se souviendra essentiellement que celle de q^* est A^{-1} .

2.2.4 Classification projective des coniques propres non vides

Dans ce paragraphe, nous montrons qu'il n'y a, à homographie près, qu'une conique propre non vide dans le plan projectif $\mathbf{P}(E)$.

2.2.23 Lemme. *Soit \bar{q} une conique propre non vide, $\Gamma = V(q)$ son ensemble de points. On a $|\Gamma| \geq 4$.*

Démonstration. Soit $a \in \Gamma$. Comme k n'est pas de caractéristique 2, son cardinal est ≥ 3 , donc le cardinal de la droite projective duale a^* des droites passant par a est ≥ 4 . Parmi ces droites, une seule est tangente à Γ (cf. 2.2.15). Les autres recoupent donc Γ en au moins trois points distincts de a .

2.2.24 Proposition.

- 1) *Soit \bar{q} une conique propre non vide, $\Gamma = V(q)$. Si a, b, d sont des points distincts de Γ et si c est le point d'intersection des tangentes à Γ en a et b , les quatre points a, b, c, d forment un repère de $\mathbf{P}(E)$.*
- 2) *Réciproquement, si a, b, c, d est un repère de E , il existe une unique conique propre \bar{q} passant par a, b, d et telle que les tangentes à $\Gamma = V(q)$ en a et b se coupent en c . Dans le repère a, b, c, d on a $q = Y^2 - XT$ à un scalaire près.*
- 3) *Soit \bar{q} une conique propre non vide, $\Gamma = V(q)$. Il existe une base de E dans laquelle q a pour expression $Y^2 - XT$, à un scalaire près. Autrement dit, Γ détermine q à un scalaire près : si on a une forme quadratique q' telle que $V(q) = V(q')$, on a $q' = \lambda q$ avec $\lambda \neq 0$.*

Démonstration. 1) Le théorème de Bézout et la définition des tangentes assurent que trois des points a, b, c, d ne sont pas alignés. On a donc bien un repère.

2) On peut choisir une base de E dans laquelle des représentants des points a, b, c, d sont donnés par $a = (0, 0, 1)$, $b = (1, 0, 0)$, $c = (0, 1, 0)$, $d = (1, 1, 1)$. Si on écrit que la conique $q = uX^2 + vY^2 + wT^2 + 2u'YT + 2v'TX + 2w'XY$ passe par a, b, d et est tangente aux droites d'équations X et T , on trouve $q = v(Y^2 - XT)$.

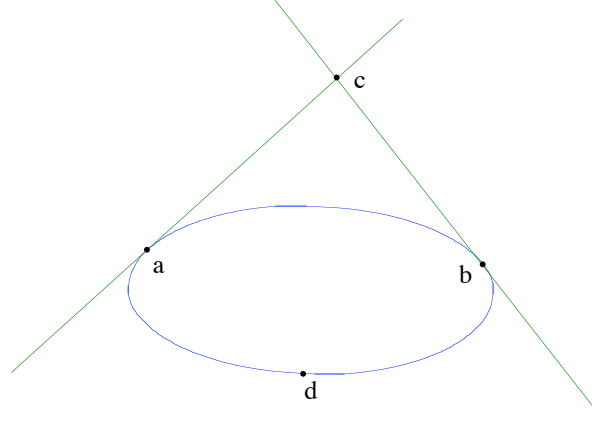


Figure 2.4: Le repère qui donne l'équation $Y^2 - XT = 0$.

3) On choisit a, b, d distincts dans $\Gamma = V(q)$. Les tangentes à Γ en a et b se coupent en c . Les points a, b, c, d forment un repère en vertu de 1) et la conclusion vient de 2).

2.2.25 Remarque. On voit ainsi que, pour les coniques propres non vides, la donnée de $\Gamma = V(q)$ équivaut à celle de la conique. On pourra donc parler de la conique Γ au lieu de la conique \bar{q} .

La proposition précédente permet de montrer le théorème principal de cette section :

2.2.26 Théorème. *Le groupe $PGL(E)$ opère transitivement sur l'ensemble des coniques propres non vides.*

Démonstration. Deux coniques propres non vides \bar{q} et \bar{q}' admettant la même équation $Y^2 - XT$ (à un scalaire près) dans deux repères convenables, cela signifie que les formes sont équivalentes à un scalaire près, d'où la conclusion (cf. 2.2.3). On notera qu'il s'agit d'un résultat algébrique bien connu sur les formes de Lorentz, cf. [Per96].

2.2.27 Remarque. Si l'on souhaite avoir une forme dont le discriminant est un carré (cf. 2.1.5) il suffit de prendre q sous la forme $XT - Y^2$.

2.2.5 Classification affine

Considérons, dans le plan projectif $\mathbf{P}(E)$ muni des coordonnées homogènes (x, y, t) une conique d'équation $q(X, Y, T) = aX^2 + bY^2 + cT^2 + 2dYT + 2eTX + 2fXY$ et soit $\Gamma = V(q)$. Si l'on prend $T = 0$ comme droite à l'infini, le plan affine Π associé est l'ensemble des points $(x, y, 1)$ et la trace de Γ sur ce plan est la courbe d'équation $q^b(x, y) = q(x, y, 1) = ax^2 + by^2 + 2fxy + 2ex + 2dy + c = 0$. C'est la conique affine associée à Γ et au choix de la droite à l'infini. Contrairement à ce qui se passe dans le cas projectif, il y a plusieurs types de coniques affines. La définition suivante va permettre au lecteur de retrouver des objets familiers :

2.2.28 Définition. Soit Γ une conique propre non vide de $\mathbf{P}(E)$, D une droite de $\mathbf{P}(E)$, choisie comme droite de l'infini et soit $\Pi = \mathbf{P}(E) - D$ le plan affine associé. On pose $\Gamma_0 = \Gamma \cap \Pi$ et on dit que Γ_0 est une conique affine de Π . On sait que $\Gamma \cap D$ est de cardinal ≤ 2 . Il y a donc trois cas :

- 1) $|\Gamma \cap D| = 2$, on dit que Γ_0 est une **hyperbole**,
- 2) $|\Gamma \cap D| = 1$, on dit que Γ_0 est une **parabole**,
- 3) $|\Gamma \cap D| = 0$, on dit que Γ_0 est une **ellipse**.

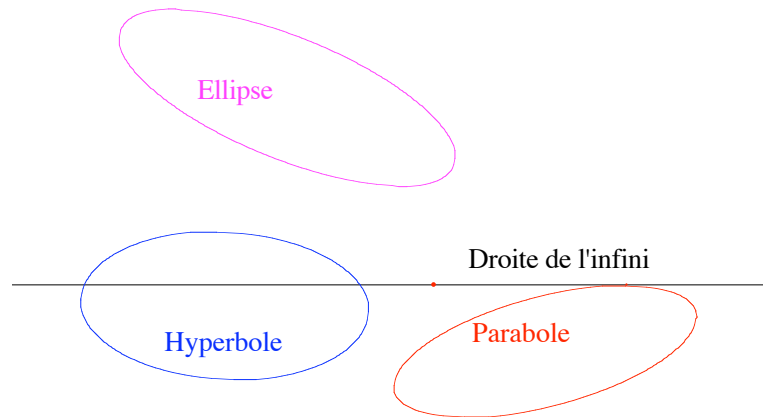


Figure 2.5: La vision projective de la classification affine.

2.2.29 Remarques.

- 1) Lorsque le corps de base est algébriquement clos, une conique affine est du type hyperbole ou parabole.
- 2) La classification affine des coniques est un peu plus délicate que leur classification projective, même dans le cas des coniques propres. En effet,

on montre aisément que deux hyperboles (resp. deux paraboles) sont dans la même orbite sous l'action du groupe affine du plan, voir exercice 2.4.2. Pour deux ellipses c'est encore vrai sur \mathbf{R} , mais c'est faux sur un corps quelconque. Par exemple, les ellipses d'équations $x^2 + y^2 = 1$ et $x^2 + 2y^2 = 1$ ne sont pas équivalentes sur \mathbf{Q} , voir exercice 2.4.4.

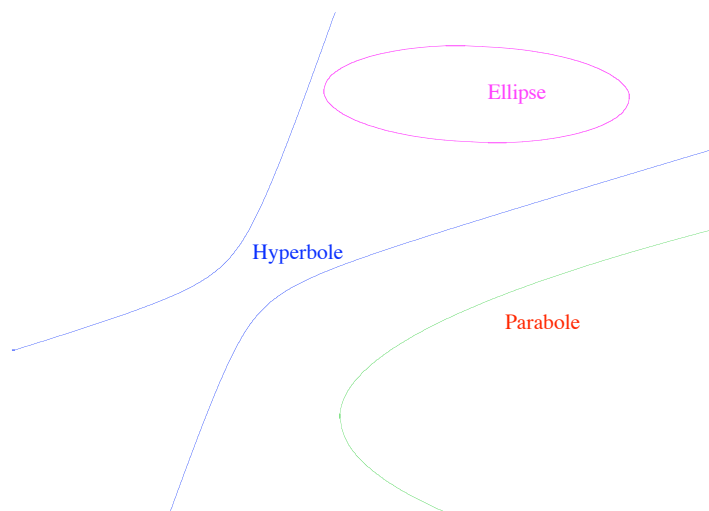


Figure 2.6: Les objets familiers.

2.2.30 Remarque. Attention, la nature d'une conique affine dépend de manière essentielle du choix de la droite à l'infini. Examinons le cas de la conique projective propre non vide Γ donnée par son équation $Y^2 - XT = 0$ et regardons sa trace sur les différents plans affines obtenus, à partir de $\mathbf{P}(E)$, en enlevant une droite "à l'infini".

Si l'on prend $T = 0$ comme droite à l'infini, le plan affine Π_1 associé est l'ensemble des points $(x, y, 1)$ et la trace de Γ sur ce plan est la courbe d'équation $x = y^2$. Le lecteur reconnaîtra bien ce qu'il a coutume d'appeler une parabole.

Si l'on prend, au contraire, $Y = 0$ comme droite à l'infini, le plan affine Π_2 associé est l'ensemble des points $(x, 1, t)$ et la trace de Γ sur ce plan est la courbe d'équation $xt = 1$: une hyperbole.

Si l'on prend, enfin, la droite $X + T = 0$ comme droite à l'infini et qu'on effectue le changement de variables : $T' = X + T, X' = X, Y' = Y$, la trace de Γ dans le plan affine Π_3 associé à $T' = 0$, i.e. le plan des $(x', y', 1)$, a pour équation $x'^2 + y'^2 - x' = 0$. Il s'agit d'une ellipse.

2.3 Conjugaison par rapport à une conique propre, pôles et polaires

La notion de conjugaison par rapport à une conique n'est rien d'autre que la traduction de l'orthogonalité pour la forme quadratique associée. Elle a un sens géométrique clair dans le cas d'une conique propre non vide, comme dans le cas d'une conique formée de deux droites. Nous verrons dans la Partie IV que cette notion est essentielle aussi dans le cas d'une forme anisotrope, qui correspond pourtant à une conique vide.

2.3.1 Définitions

2.3.1 Définition. Soit \bar{q} une conique et soient $a, b \in \mathbf{P}(E)$. On dit que a, b sont conjugués pour \bar{q} si on a $\varphi(a, b) = 0$, où φ désigne la forme polaire de q .

2.3.2 Remarques.

- 1) On notera qu'on a commis les abus de langage annoncés plus haut. Si F est un sous-espace projectif de $\mathbf{P}(E)$, image d'un sous-espace vectoriel V de E , on notera d'ailleurs F^\perp l'image du sous-espace V^\perp , ensemble des points conjugués de tous les points de F .
- 2) Si m est sur Γ , il est conjugué de lui-même car on a $q(m) = \varphi(m, m) = 0$.
- 3) Si m est un point double de q (i.e. l'image d'un vecteur du noyau de q), il est conjugué de tout point du plan.
- 4) Si $\Gamma = V(q)$ est non vide, on dira aussi que les points sont conjugués par rapport à Γ .

2.3.3 Proposition-Définition. Soit \bar{q} une conique.

- 1) Soit m un point qui n'est pas un point double de \bar{q} . L'ensemble des conjugués de m est une droite appelée **polaire** de m par rapport à \bar{q} . On la note m^\perp .
- 2) Soit D une droite qui ne contient pas de point double de \bar{q} . Il existe un unique point conjugué de tous les points de D , le **pôle** de D . On le note D^\perp .

Démonstration. Cela résulte de 1.2.2 et 1.2.5.5.

2.3.4 Remarques.

- 1) La propriété dite traditionnellement de "réciprocité polaire" : si a est sur la polaire de b , alors b est sur la polaire de a , n'est rien d'autre que la symétrie de la relation de conjugaison qui provient du fait que la forme φ est symétrique.
- 2) L'équation de la polaire de a est $\varphi(a, m) = 0$. Si on a $q(x, y, t) = \alpha x^2 +$

$\beta y^2 + \gamma t^2 + 2\delta yt + 2\epsilon tx + 2\eta xy = 0$, et si on pose $m = (x, y, t)$ et $a = (u, v, w)$, cette équation s'écrit, comme celle de la tangente :

$$\alpha ux + \beta vy + \gamma wt + \delta(wy + vt) + \epsilon(ut + wx) + \eta(vx + uy) = 0.$$

3) Si a n'est pas un point double, il est sur sa propre polaire si et seulement si c'est un point de $V(q)$. La polaire est alors la tangente en a .

2.3.5 Théorème. *Soit \bar{q} une conique propre. L'application qui à un point associe sa polaire est une homographie de $\mathbf{P}(E)$ dans $\mathbf{P}(E^*)$ dont la réciproque est l'application qui à une droite associe son pôle. En particulier, trois points sont alignés si et seulement si leurs polaires sont concourantes.*

Démonstration. Cela résulte de 1.2.8 : l'orthogonalité est une homographie.

On peut caractériser aussi en termes de pôle le cas où une droite coupe une conique en deux points :

2.3.6 Proposition. *Soit $\Gamma = V(q)$ une conique propre et D une droite de pôle a . La droite coupe la conique en deux points distincts si et seulement si $-\Delta(q)q(a)$ est un carré non nul. Si q^* est la forme duale et si D a pour équation l , la condition signifie aussi que $-\Delta(q^*)q^*(l)$ est un carré.*

Démonstration. Cela vient de 2.2.14 puisqu'on a $\Delta(q) = q(a)\Delta(q|_F)$ si D est l'image du plan vectoriel F . L'assertion sur la forme duale vient des formules suivantes : $l = \varphi_a$, $q^*(l) = q(a)$ (cf. 1.4.2) et $\Delta(q^*) = \Delta(q)^{-1} = \Delta(q)/\Delta(q)^2$ (cf. 1.4.1).

2.3.2 Polaire et division harmonique

Le théorème suivant est encore une conséquence de 1.2.8 et des résultats de la partie I :

2.3.7 Théorème. *Soit \bar{q} une conique et D une droite projective image du plan vectoriel F . On suppose que D n'est pas une tangente à \bar{q} , i.e. que $q|_F$ est non dégénérée. L'application qui à un point m de D associe l'unique point de D conjugué par rapport à \bar{q} est une involution de D .*

Démonstration. Comme D n'est pas tangente, m n'est pas un point double, de sorte que m^\perp est une droite, et cette droite est différente de D , toujours parce que D n'est pas tangente. L'intersection $D \cap m^\perp$ est donc réduite à un point m' .

L'application $m \mapsto m^\perp$ est une homographie par 1.2.8 et il en est de même de $m^\perp \mapsto m'$ (car cette application est une incidence, cf. Partie I ??). Le fait que, pour m' donné, il y ait un unique point m de D conjugué de m' montre que l'application $m \mapsto m'$ est une involution.

2.3.8 Corollaire. Soit \bar{q} une conique et soient $a, b \in \mathbf{P}(E)$ deux points distincts, non situés sur $\Gamma = V(q)$. On suppose que la droite (ab) coupe Γ en u et v . Alors, a et b sont conjugués par rapport à \bar{q} si et seulement si on a $\llbracket a, b, u, v \rrbracket = -1$.

Démonstration. Dans l'involution précédente, les points u et v sont les points fixes (car ils sont conjugués d'eux mêmes). L'assertion résulte alors de ??, partie I.

2.3.3 Constructions de la polaire

Nous donnons ci-dessous quelques constructions de la polaire d'un point m . Lorsqu'on dispose des tangentes issues de m la construction est immédiate (voir aussi 2.3.12) :

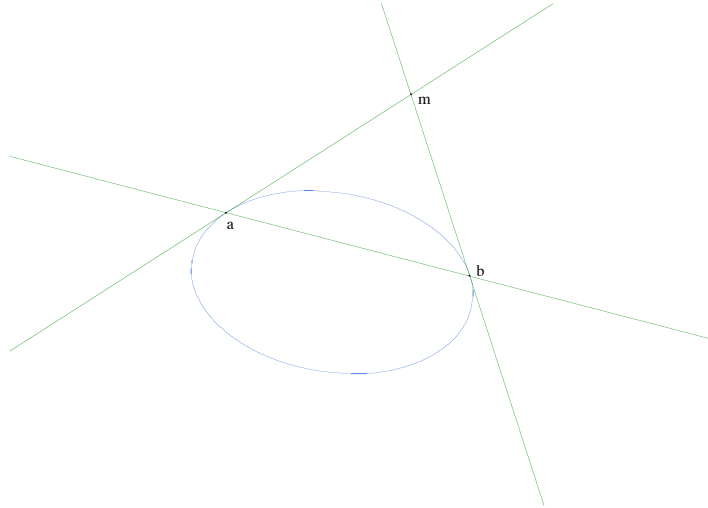


Figure 2.7: Première construction de la polaire.

2.3.9 Proposition. Soit \bar{q} une conique propre et $\Gamma = V(q)$. Soit m un point non situé sur Γ . On suppose qu'on peut mener deux tangentes à Γ passant par m qui touchent Γ en a et b . Alors la polaire de m est la droite (ab) .

Démonstration. Cela résulte de 2.2.18 et de 2.3.4.2.

Dans le cas d'une conique dégénérée en deux droites, la polaire a déjà été vue :

2.3.10 Proposition. Soit \bar{q} une conique dégénérée, avec $\Gamma = V(q)$ réunion de deux droites D_1, D_2 et soit $d \notin D_1 \cup D_2$. Alors la polaire de d par rapport à Γ est la polaire de d par rapport aux deux droites au sens de Partie I, ??.

Démonstration. Cela résulte de 2.3.8 et de Partie I, ??.

Enfin, le cas général se ramène à celui d'une conique dégénérée :

2.3.11 Proposition. *Soit \bar{q} une conique propre non vide et soit $\Gamma = V(q)$. Soit $d \notin \Gamma$. On mène deux droites A, B passant par d qui coupent respectivement Γ en a, a' et b, b' . Soit o (resp. u) le point d'intersection des droites (ab) et $(a'b')$ (resp. (ab') et $(a'b)$). Alors, la polaire de d par rapport à \bar{q} est la droite (ou) .*

Démonstration. En vertu de Partie I, ??, la polaire de d par rapport aux droites (oa) et (oa') est la droite (ou) . Il en résulte qu'on a $[[d, \alpha, a, a']] = [[d, \beta, b, b']] = -1$ (Partie I, ??). Avec 2.3.8, on en déduit que α, β sont sur la polaire de d par rapport à Γ et cette polaire est donc $(\alpha\beta) = (ou)$.

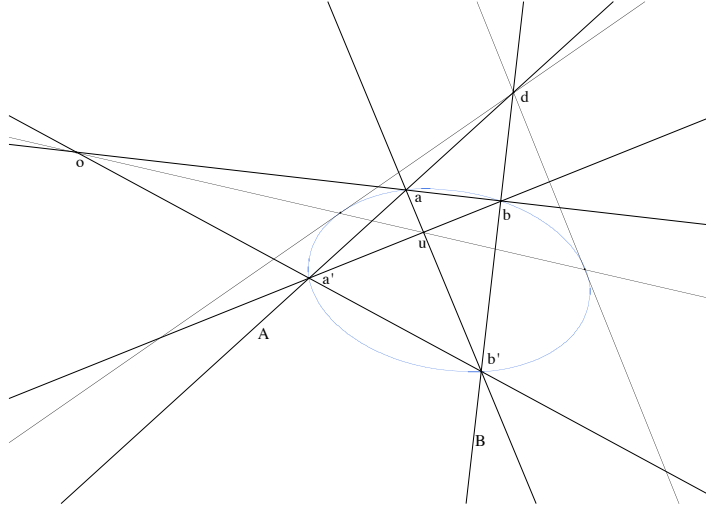


Figure 2.8: Deuxième construction de la polaire.

2.3.12 Remarque. La construction précédente fournit une construction des tangentes à Γ issues de d : ce sont les droites qui joignent d aux points d'intersection de (ou) et de Γ .

2.3.4 Triangle autopolaire

2.3.13 Définition. *Soit \bar{q} une conique. On appelle **triangle autopolaire** un triangle a, b, c tels que les points a, b, c soient deux à deux conjugués par rapport à \bar{q} .*

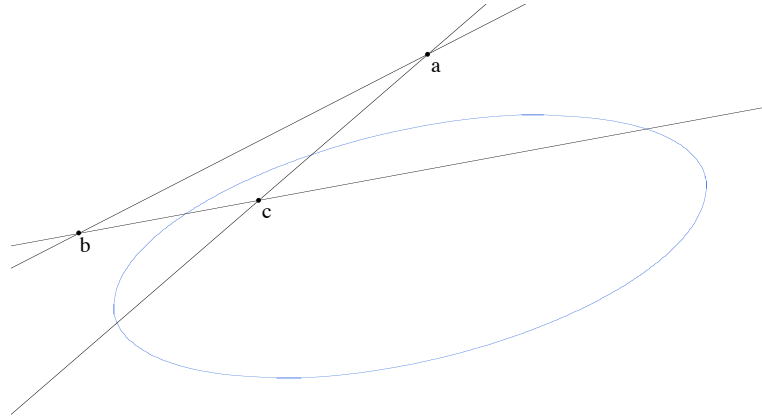


Figure 2.9: Le triangle abc est autopolaire.

2.3.14 Remarque. Un triangle autopolaire est l'image d'une base orthogonale (et il existe donc de tels triangles de premier sommet a quelconque, $a \notin V(q)$). Bien entendu la polaire de chaque sommet d'un triangle autopolaire est le côté opposé. Pour construire un tel triangle on prend un point $a \notin \Gamma$ quelconque, on trace sa polaire A , on prend un point b sur A et on trouve c à l'intersection des polaires de a et b .

2.3.5 Quelques applications affines des polaires

Même si on s'intéresse exclusivement aux coniques affines, le passage par le plan projectif peut s'avérer extrêmement fructueux. Nous donnons ici quelques applications des pôles et polaires dans le cadre de la géométrie affine. Voir aussi, par exemple, l'exercice 2.4.7. Le lecteur qui souhaite en savoir plus sur le sujet consultera [Ber90]. Dans ce paragraphe, on travaille dans un plan affine X , complémentaire de la droite D_∞ de $\mathbf{P}(E)$.

Centre et diamètres d'une conique affine

2.3.15 Proposition-Définition. Soit \bar{q} une conique propre non vide, $\Gamma = V(q)$. On suppose que la conique n'est pas une parabole.

Le pôle o de la droite D_∞ est un point du plan affine appelé **centre** de la conique. Le point o est centre de symétrie affine de Γ , c'est-à-dire qu'il existe une involution σ_o qui fixe o et les points de D_∞ et qui laisse stable Γ . Si a est un point de Γ , la droite (oa) recoupe Γ en $b = i(a)$ et o est le milieu de $[a, b]$. On dit que Γ est une conique **à centre**.

2) Les droites passant par o sont appelées **diamètres** de Γ . Si D, D' sont deux

diamètres, on dit qu'ils sont **conjugués** si leurs points à l'infini le sont. Les diamètres de Γ sont axes de symétries affines de Γ de direction le diamètre conjugué.

Démonstration. 1) Le pôle de la droite de l'infini n'est pas sur cette droite (sinon celle-ci serait tangente en vertu de 2.3.4.3 et la conique serait une parabole). L'involution i est l'homographie associée à la symétrie (orthogonale relativement à q) vectorielle dont les espaces propres (orthogonaux) sont le plan E^+ dont l'image est D_∞ et la droite E^- qui s'envoie sur o . L'assertion sur les milieux résulte de 2.3.8 et de Partie I ??.

2) Soit D un diamètre, qui coupe D_∞ en d et soit δ le pôle de D , qui est un point de D_∞ par la réciprocity polaire. L'assertion signifie que si on considère une droite Δ de direction δ , elle coupe Γ en deux points a, b dont le milieu m est sur D . C'est simplement le fait que le birapport $\llbracket a, b, m, \delta \rrbracket$ vaut -1 , voir 2.3.8.

2.3.16 Remarque. Dans un repère affine formé du centre et de deux diamètres conjugués, l'équation de la conique q est de la forme $q(x, y) = ax^2 + by^2 + c$, voir exercice 2.4.3. Pour une construction du centre voir exercice 2.4.9.

Application aux tangentes à la parabole

Nous donnons dans ce paragraphe une application des polaires et de leurs liens avec les tangentes pour établir un résultat sur les tangentes à la parabole dans le plan affine. La proposition suivante est la clé de la quadrature de la parabole telle qu'Archimède l'a réalisée.

Dire qu'une conique P est une parabole signifie qu'elle a un unique point à l'infini ω et qu'elle est tangente à D_∞ en ce point, cf. 2.2.28. On dira (en anticipant sur une notion euclidienne) que les droites $(a\omega)$ avec $a \in X$ sont les "parallèles à l'axe" de la parabole.

2.3.17 Proposition. Soit P une parabole, ω son point à l'infini et soient a, b deux points de P . Les tangentes à P en a et b se coupent en c . Soit Δ la droite $(c\omega)$ (c'est-à-dire, en termes affines, la parallèle à l'axe de P passant par c). Elle coupe P en m en (ab) en n . On a les propriétés suivantes :

- 1) m est le milieu de $[cn]$,
- 2) n est le milieu de $[ab]$,
- 3) la tangente à P en m est parallèle à (ab) .

Démonstration.

1) Il résulte de 2.3.9 que la polaire de c est la droite (ab) et c'est le lieu des conjugués harmoniques de c par rapport à P en vertu de 2.3.8. Comme

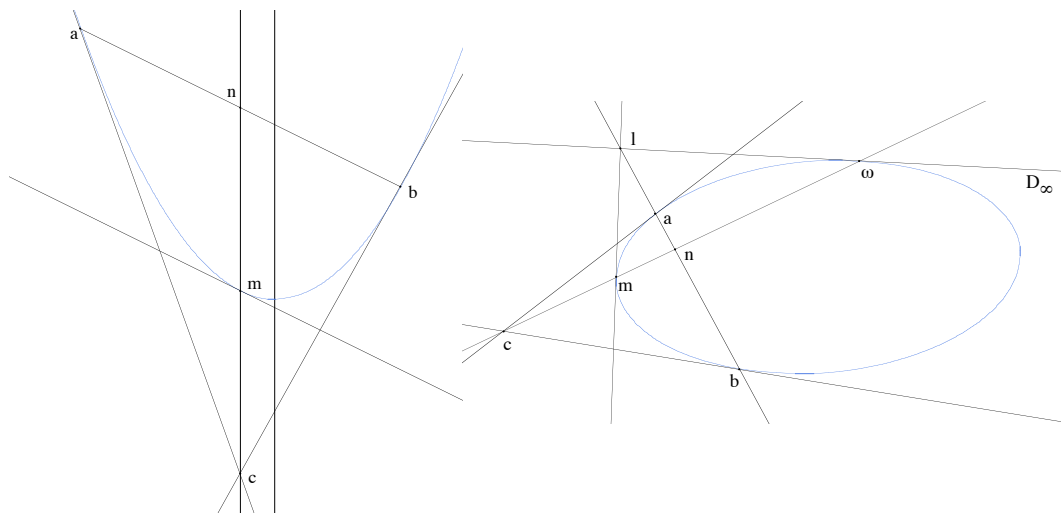


Figure 2.10: Archimède : versions affine et projective.

la sécante (cm) coupe P en ω on a $\llbracket c, n, m, \omega \rrbracket = -1$ ce qui signifie que m est milieu de $[cn]$, puisque ω est à l'infini (cf. Partie I ??).

2) Soit l le point à l'infini de (ab) . Montrons que la polaire de l est (nc) . Comme l est sur la polaire de c , les points l et c sont conjugués et c est sur la polaire de l . Comme la droite de l'infini est tangente à P en ω puisque P est une parabole, ω est aussi sur la polaire. La polaire de l est donc bien $(c\omega)$. On en déduit $\llbracket a, b, n, l \rrbracket = -1$ en vertu de 2.3.8, ce qui montre que n est le milieu de $[ab]$.

3) La construction de la polaire de l montre que les deux tangentes issues de l sont $(l\omega)$ et (lm) , de sorte que la tangente en m passe par l , i.e. est parallèle à (ab) .

2.3.18 Remarques. 1) Pour voir comment cette proposition permet de réaliser la quadrature de la parabole, avec exactement la même preuve qu'Archimède, voir [Arc60], [RD89b] Ch. VI, 27-ième leçon, §251 ou [Per05].

2) Bien entendu Archimède ne prouvait pas ainsi la proposition ! Il en attribue partiellement la paternité à Euclide et en donne d'autres preuves par des moyens mécaniques (des arguments de levier). On peut aussi en donner des démonstrations euclidiennes en utilisant foyer et directrice (voir [RD89b] *loc. cit.*) ou analytiques en prenant $y = x^2$ comme équation de P .

2.4 Exercices

2.4.1 Classification

2.4.1 Exercice. On suppose qu'on a $\Delta(q) = -1$ dans k^*/k^{*2} . Montrer que si D coupe Γ en deux points alors $q^*(D)$ est un carré.

2.4.2 Exercice. Le but de cet exercice est de montrer que deux hyperboles (resp. deux paraboles) quelconques sont échangées par une application affine. On travaille dans $\mathbf{P}(E)$ muni d'une droite D_∞ et on appelle X le plan affine associé.

1) Soit u une homographie qui laisse stable D_∞ . Montrer que $u|_X$ est une application affine (on utilisera la matrice de u et on montrera que $u|_X(x, y)$ est de la forme $(ax + by + \alpha, cx + dy + \beta)$).

2) Soient C, C' deux hyperboles de points à l'infini a, b et a', b' respectivement. On appelle c (resp. c') les points d'intersection des tangentes à C en a, b (resp. à C' en a', b'). Soient $d \in C$, $d' \in C'$ deux points distincts des précédents. Conclure en notant qu'il existe une homographie qui envoie a, b, c, d sur a', b', c', d' .

3) Traiter de même le cas des paraboles.

2.4.3 Exercice. Soient Γ une conique affine, o son centre, D et Δ deux diamètres conjugués.

1) Montrer que l'équation de Γ dans un repère affine d'origine o et d'axes portés par D et Δ est de la forme $Ax^2 + By^2 + C = 0$. (Prendre un repère projectif dont les trois premiers points sont o et les points à l'infini d et δ des diamètres et utiliser 2.3.4.2.)

2) Si Γ est une ellipse (resp. une hyperbole), montrer qu'on peut supposer que son équation est de la forme $Ax^2 + By^2 = 1$ avec $A, B \neq 0$ et $A/B \notin k^{*2}$ (resp. $A/B \in k^{*2}$). Si k est le corps des réels, montrer qu'on peut supposer $A = 1/a^2$ et $B = 1/b^2$ (resp. $B = -1/b^2$).

2.4.4 Exercice. Soient Γ, Γ' deux coniques d'équations $Ax^2 + By^2 = 1$ et $A'x^2 + B'y^2 = 1$ avec A, B, A', B' non nuls.

1) Montrer que si une application affine u envoie Γ' sur Γ elle conserve l'origine $(0, 0)$ (penser aux centres).

2) On écrit u sous la forme $u(x, y) = (\alpha x + \beta y, \gamma x + \delta y)$. Montrer que u envoie Γ' sur Γ si et seulement si on a $A' = A\alpha^2 + B\gamma^2$, $B' = A\beta^2 + B\delta^2$, $A\alpha\beta + B\gamma\delta = 0$.

3) On suppose $k = \mathbf{R}$. Montrer que deux ellipses quelconques sont équivalentes sous l'action du groupe affine du plan.

4) On suppose $k = \mathbf{Q}$ et on considère les ellipses d'équations $x^2 + y^2 = 1$ et $x^2 + 3y^2 = 1$. Montrer qu'elles ne sont pas équivalentes sous l'action du groupe affine du plan. (En réduisant au même dénominateur et en regardant les congruences modulo 4, on montrera que l'équation $\beta^2 + \delta^2 = 3$ n'a pas de solution dans \mathbf{Q} .)

Même question en remplaçant $x^2 + 3y^2 = 1$ par $x^2 + 2y^2 = 1$.

2.4.2 Propriétés affines des coniques

2.4.5 Exercice. On travaille dans le plan affine $X = \mathbf{P}(E) - D_\infty$. Soit Γ une conique de X , soient a, b deux points distincts de X et m leur milieu. On trace deux droites passant par m qui coupent Γ respectivement en p, q et r, s . Soit u (resp. v) le point d'intersection de (ab) et de (ps) (resp. (qr)). Montrer³ que m est le milieu de u, v . (Indication : si on appelle respectivement e et f les points d'intersection de (ps) et (qr) et de (pr) et (qs) , on montrera que la droite (ef) est la polaire de m à la fois par rapport à la conique et par rapport à la paire de droites (ps) et (qr) et on montrera que le point à l'infini de (ab) est aussi sur (ef) .)

2.4.6 Exercice. On se propose de construire (par exemple à l'aide de la macro “conique” de Cabri-géomètre), une parabole P dont on connaît trois points a, b, c et la direction de l'axe (c'est-à-dire le point de contact de P et de D_∞).

1) Montrer que la parabole P existe et est unique.

2) Montrer que, si a, b sont deux points d'une parabole P , et si D est une droite passant par le milieu de $[a, b]$ et parallèle à l'axe de P , D est axe de symétrie oblique de P dans la direction (ab) .

3) La macro “coniques” de Cabri construit une conique dont on connaît cinq points. Construire la parabole P en construisant deux nouveaux points de P (utiliser le point 2) en introduisant les milieux de $[a, b]$ et $[b, c]$).

2.4.7 Exercice. Cet exercice se propose de montrer une propriété affine de l'hyperbole par des voies projectives. Soit H une hyperbole, d, d' ses points à l'infini, D, D' les tangentes à H en ces points (les “asymptotes” de H).

1) Montrer que D et D' se coupent au centre o de H . Montrer que, dans un repère d'origine o et d'axes portés par les asymptotes, l'équation affine de H est de la forme $xy = k$, avec $k \neq 0$.

³Cet exercice m'a été suggéré par Jean-Pierre Kahane. Il se trouve dans le livre de David Ruelle (*L'étrange beauté des mathématiques*, Odile Jacob, 2008) qui l'énonce dans le cas du cercle mais en donne une démonstration projective.

2) Soit m un point de H . La tangente en m coupe les asymptotes en a et a' . Montrer que m est le milieu de $[a, a']$. (Soient b le point à l'infini de la tangente et c celui de (om) . On montrera successivement :

- que la polaire de b par rapport à H est la droite (om) ,
- qu'on a $\llbracket b, c, d, d' \rrbracket = -1$,
- que (om) est aussi la polaire de b par rapport à la conique dégénérée $D \cup D'$.)

2.4.8 Exercice. Soit Γ une conique du plan affine et soit abc un triangle inscrit dans Γ . Les tangentes en b et c à Γ se coupent en d et la parallèle à la tangente en a passant par d coupe respectivement (ab) en e et (ac) en f . Montrer que d est le milieu de (ef) . (On considérera le point p , intersection de la tangente en a avec (bc) , et sa polaire par rapport à Γ et par rapport aux droites (ab) et (ac) .)

2.4.9 Exercice. 1) On se donne une conique affine Γ . Construire le centre o de Γ (on établira la propriété suivante : si deux droites parallèles coupent Γ en a, b et a', b' respectivement, la droite qui joint les milieux de $[a, b]$ et $[a', b']$ passe par o).

2) On travaille dans le plan réel euclidien et on considère une ellipse Γ . Construire⁴ les axes de symétrie orthogonale de Γ (on tracera un cercle de centre o qui coupe l'ellipse en quatre points).

2.4.10 Exercice. Dans cet exercice on suppose $k = \mathbf{R}$ ou \mathbf{C} . Soit Γ une conique propre non vide et abc un triangle autopolaire.

Montrer que deux au moins des droites (bc) , (ca) , (ab) coupent Γ en deux points⁵. (Écrire une équation de Γ sous la forme $X^2 + Y^2 - T^2 = 0$ dans un repère comprenant les points a, b, c .)

⁴Cet exercice est inspiré d'une question de Claire Alamichel, fille de ma collègue Anne Broise, qui était alors en sixième. Son professeur leur avait demandé de construire les axes de symétrie d'une ellipse et Claire – bon sang ne saurait mentir – ne se satisfaisait pas de les tracer à l'œil.

⁵L'exemple de la conique d'équation $X^2 + Y^2 - 2T^2 = 0$ montre que la propriété est fausse sur le corps \mathbf{Q} .

Chapitre 3

La conique vue comme une droite projective

Dans ce chapitre nous allons montrer qu'il y a au moins trois bonnes raisons de voir une conique propre non vide comme une droite projective : l'existence d'un paramétrage par une droite, la définition du birapport de quatre points et l'isomorphisme du groupe des homographies qui conservent la conique avec le groupe projectif de la droite : $PGL(2, k)$. Nous étudierons en particulier les involutions qui conservent une conique et leurs points de Frégier avec des applications à la fois géométriques et algébriques et nous aborderons trois thèmes historiques : un théorème de Newton, un résultat de Poncelet et une généralisation du théorème de Pascal qui donnera en particulier la loi de groupe sur une cubique plane.

Dans tout ce chapitre, Γ est une conique propre non vide d'équation q .

3.1 Paramétrisation d'une conique propre non vide, birapport

3.1.1 Définition du paramétrage

Soit $a \in \Gamma$. Rappelons que l'on désigne par a^* l'ensemble des droites passant par a , qui est muni d'une structure de droite projective, voir Partie I ???. On définit une application bijective $\pi_a : \Gamma \rightarrow a^*$ en associant à un point m de Γ la droite (am) si m est distinct de a et la tangente en a si m est égal à a . La réciproque de cette application associe à une droite D passant par

a le point a si D est la tangente à Γ en a et l'autre point d'intersection de D et Γ sinon (voir 2.2.16). Cette application va permettre de munir Γ d'une structure de droite projective en l'identifiant à la droite projective a^* . Encore faut-il montrer que cette structure ne dépend pas du choix du point a , c'est l'objet du théorème suivant :

3.1.1 Théorème. *Avec les notations ci-dessus, si a et b sont deux points de Γ , l'application $f = \pi_b \circ \pi_a^{-1}$ est une homographie de a^* dans b^* .*

Démonstration. Si Δ est une droite passant par a qui recoupe la conique en p , l'application f associe à $\Delta = (ap)$ la droite (bp) . Soit ω le pôle de la droite (ab) et soit D une droite passant par ω , ne passant pas par a et b . Soit x un point de D . Considérons l'application g de D dans D obtenue de la façon suivante. On effectue d'abord l'incidence $x \mapsto (ax)$ de D dans a^* . Si p est le point d'intersection de Γ et (ax) autre¹ que a , on effectue ensuite l'application f de a^* dans b^* , qui à $(ax) = (ap)$ associe (bp) . Enfin on effectue l'incidence de b^* dans D qui à (bp) associe le point d'intersection y de cette droite et de D . Comme les incidences sont des homographies, il suffit de montrer que l'application g qui à x associe y est une homographie de D .

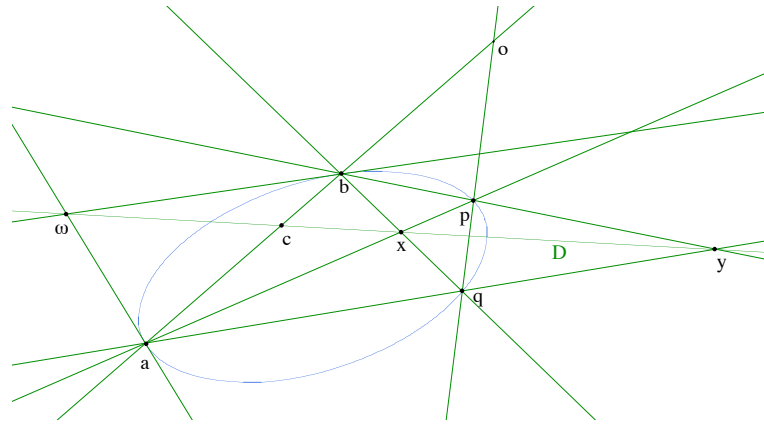


Figure 3.1: La preuve de 3.1.1

Comme g fixe les points d'intersection u, v de D et Γ (s'il en existe) et qu'elle échange ω et le point c , intersection de D et (ab) , qui est conjugué de ω et on peut subodorer que g est simplement la restriction à D de la conjugaison par rapport à la conique. On montre effectivement :

3.1.2 Lemme. *Les points x et y sont conjugués par rapport à Γ .*

¹Sauf si (ax) est tangente à Γ en a , auquel cas p est en a .

Appelons o le pôle de D . Comme ω est sur D , o et ω sont conjugués, donc o est sur (ab) . Reprenons les notations x, p, y ci-dessus. Soit q le point d'intersection de Γ et (op) autre que p . La construction de la polaire (cf. 2.3.11) montre que le point d'intersection x' de (ap) et (bq) est sur la polaire de o , i.e. sur D . Or, x aussi est à la fois sur D et sur (ap) . On a donc $x = x'$ et x est sur (bq) . De même, le point d'intersection de (aq) et (bp) est sur la polaire de o et c'est donc y . Mais alors, la construction de la polaire de y par rapport à Γ montre que x est sur cette polaire, donc conjugué de y , cqfd.

Le théorème est alors immédiat. En effet, le lemme montre que l'application g est l'application d'orthogonalité pour la forme $q|_D$. Mais on sait que cette application est une homographie, cf. 1.2.8.

3.1.3 Remarque. On notera dans la configuration précédente le rôle capital joué par le triangle autopolaire oxy .

3.1.4 Proposition-Définition. Soient $a, b, c, d \in \Gamma$ quatre points distincts et soit $m \in \Gamma$. Alors, le birapport des quatre droites² $(ma), (mb), (mc), (md)$ de la droite duale m^* est indépendant du point m . On l'appelle **birapport** des quatre points de Γ et on le note $\llbracket a, b, c, d \rrbracket$.

Démonstration. Cela résulte aussitôt du théorème précédent.

3.1.5 Corollaire. Le groupe G des bijections de la conique Γ qui conservent le birapport est isomorphe au groupe $PGL(2, k)$ des homographies d'une droite projective.

Démonstration. On choisit un point $m \in \Gamma$. L'application $g \mapsto \pi_m f \pi_m^{-1}$ est un isomorphisme de G sur le groupe des bijections de m^* qui conservent le birapport, et ce groupe est le groupe des homographies en vertu de Partie I ??.

3.1.2 Calcul explicite du paramétrage

On peut supposer que la conique a pour équation $q(X, Y, T) = Y^2 - XT$ et prendre $a = (0, 0, 1)$. Alors, une droite D de a^* a pour équation $\mu X - \lambda Y = 0$, avec λ, μ non tous deux nuls. On cherche les points d'intersection de Γ et D , donnés par le système :

$$\mu x - \lambda y = 0, \quad y^2 - xt = 0.$$

²Avec la sempiternelle convention que si on a, par exemple, $m = a$, la droite (ma) est la tangente en m à Γ .

Supposons d'abord $\lambda \neq 0$. On obtient la solution $x = 0$ qui correspond au point a et, si x est non nul, on a $y = \frac{\mu x}{\lambda}$ et $t = \frac{\mu^2 x}{\lambda^2}$. Comme les coordonnées (x, y, t) sont homogènes, on peut prendre $x = \lambda^2$ et on trouve $m = (\lambda^2, \lambda\mu, \mu^2)$. Le cas $\lambda = 0$ correspond au cas où D est tangente en $a = (0, 0, 1)$ et on constate que ce point est aussi de la forme annoncée. L'application π_a^{-1} de a^* dans Γ est donc donnée par la formule $\pi_a^{-1}(\lambda, \mu) = (\lambda^2, \lambda\mu, \mu^2)$.

3.1.6 Remarques.

- 1) On peut utiliser ce calcul explicite pour donner une autre preuve de 3.1.1, voir exercice 3.6.1.
- 2) Lorsque le corps de base est \mathbf{R} ou \mathbf{C} l'application π_a^{-1} de $\mathbf{P}^1(k)$ sur Γ est continue, comme on le voit sur la formule ci-dessus. Comme la droite projective est compacte, π_a^{-1} est un homéomorphisme. Une conique propre réelle est ainsi homéomorphe à une droite projective réelle (donc à un cercle) et une conique propre complexe à une droite projective complexe (donc à une sphère) voir Partie I ??.

3.1.3 Traduction tangentielle : birapport de quatre tangentes

Les résultats précédents, appliqués à la conique duale $\overline{q^*}$ (voir 2.1.1 et 2.2.21) permettent de définir le birapport de quatre tangentes à une conique :

3.1.7 Proposition-Définition. Soient Γ une conique propre, A, B, C, D quatre tangentes à Γ , distinctes, et soit M une tangente à Γ . On appelle a, b, c, d les points d'intersection³ de M et de A, B, C, D respectivement. Alors, le birapport $\llbracket a, b, c, d \rrbracket$ est indépendant de M . On l'appelle **birapport des quatre tangentes** à Γ et on le note $\llbracket A, B, C, D \rrbracket$.

Démonstration. C'est 3.1.4 appliqué à la conique duale $\overline{q^*}$.

3.1.8 Proposition. Soit Γ une conique propre, a, b, c, d quatre points de Γ et A, B, C, D les tangentes en ces points. On a $\llbracket a, b, c, d \rrbracket = \llbracket A, B, C, D \rrbracket$.

Démonstration. Il suffit de noter que l'application de Γ dans Γ^* qui à un point a associe la tangente A à Γ en a est la restriction à Γ de l'homographie $a \mapsto a^\perp$, voir 2.3.5.

³Si M est, par exemple, égale à A , le point a est le point de contact de A et de Γ .

On peut aussi faire le calcul, qui est très simple. On suppose que la conique Γ a pour équation $Y^2 - XT$ et on utilise le paramétrage $(\lambda^2, \lambda\mu, \mu^2)$. La conique duale a pour équation $Y^2 - 4XT = 0$ que l'on paramètre par $(\alpha^2, 2\alpha\beta, \beta^2)$. On vérifie que la tangente au point de paramètre (λ, μ) a pour paramètre $(\mu, -\lambda)$. Comme l'application $(\lambda, \mu) \mapsto (\mu, -\lambda)$ est une homographie, on a le résultat.

3.1.4 Application : le théorème de Pascal

Il s'agit de l'analogue du théorème de Pappus, mais avec une conique propre en lieu et place d'une conique dégénérée en deux droites. Maintenant que nous disposons du birapport, la démonstration est essentiellement la même.

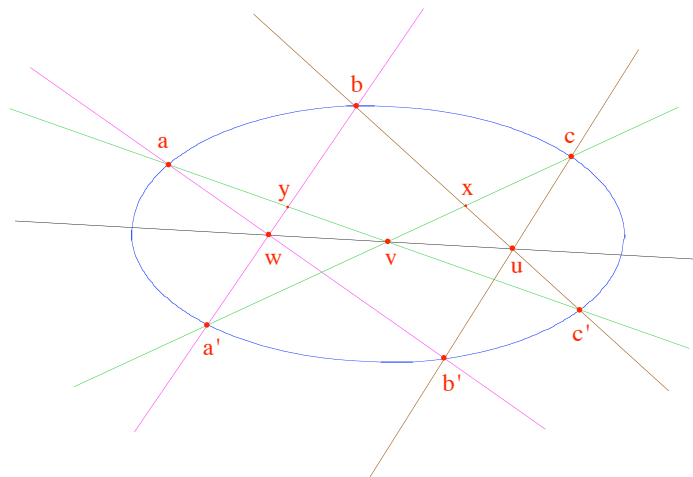


Figure 3.2: Le théorème de Pascal

3.1.9 Théorème. Soit Γ une conique propre non vide et soient a, b, c, a', b', c' six points distincts de Γ (un hexagone). On appelle respectivement u, v, w les points d'intersection des droites (bc') et $(b'c)$, (ca') et $(c'a)$, (ab') et $(a'b)$. Alors, u, v, w sont alignés.

Démonstration. Appelons x (resp. y) le point d'intersection de $(a'c)$ et (bc') (resp. de $(a'b)$ et (ac')). On considère la perspective p_v de centre v de (bc') sur $(a'b)$. Elle envoie donc b sur b , x sur a' et c' sur y . Les points u, v, w sont alignés si cette perspective envoie aussi u sur w . Pour voir cela il suffit de montrer l'égalité de birapports $\llbracket b, c', x, u \rrbracket = \llbracket b, y, a', w \rrbracket$. Mais, par incidence on a $\llbracket b, c', x, u \rrbracket = \llbracket (cb), (cc'), (cx), (cu) \rrbracket$ et, par définition du birapport

sur Γ , ce birapport est encore égal à $\llbracket b, c', a', b' \rrbracket$, ou encore, en vertu de 3.1.4 à $\llbracket (ab), (ac'), (aa'), (ab') \rrbracket$, c'est-à-dire, en coupant ces droites par $(a'b)$, à $\llbracket b, y, a', w \rrbracket$, cqfd.

3.1.10 Remarques.

1) Le théorème de Pascal vaut encore si deux (voire plus) des points de l'hexagone sont confondus, à condition de remplacer la droite qui les joint par la tangente, voir exercice 3.6.2. Cela fournit une construction de la tangente à Γ en un de ses points a . Pour cela on prend quatre autres points b, c, a', c' de Γ et on pose $b' = a$. On construit les points v et w intersections respectives de (ac') et $(a'c)$ et de (bc') et $(b'c)$. La droite (vw) coupe alors (ba') en u et la tangente en a est la droite (au) , voir fig.3.3.

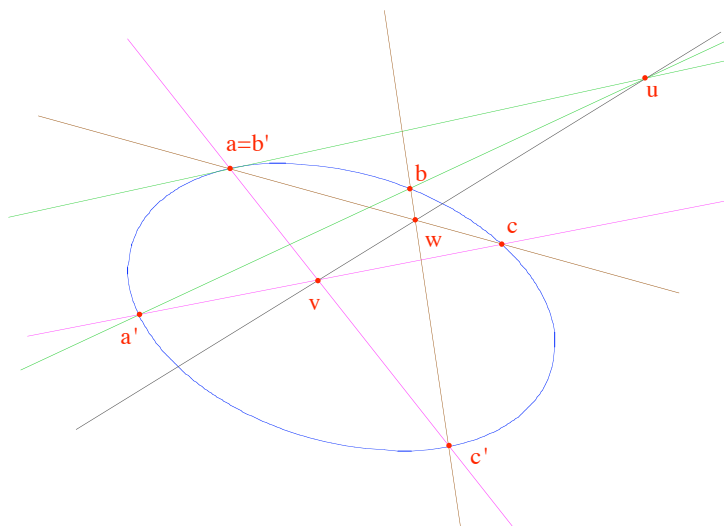


Figure 3.3: Utilisation de Pascal pour la construction d'une tangente.

2) Le lecteur énoncera et prouvera le théorème dual (dit de Brianchon) avec six tangentes à Γ .

3.2 Le groupe de la conique

3.2.1 Diverses formes du groupe d'une conique

La problématique de cette étude est la suivante. Le groupe $PGL(E)$ des homographies du plan opère sur l'espace $\mathbf{P}(Q)$ des coniques, cf. 2.2.1. On a vu que les coniques propres non vides forment une seule orbite dans cette action (cf. 2.2.26). La question est maintenant de déterminer le stabilisateur

d'une conique propre non vide \bar{q} , donc de trouver les applications linéaires $u \in GL(E)$ qui transforment la forme q en une forme proportionnelle : $q \circ u^{-1} = \lambda q$. On a vu, cf. 1.3.6, que ce sont les similitudes, éléments du groupe $GO(q)$. Le stabilisateur de \bar{q} est donc l'image de ce groupe dans le groupe des homographies, i.e. le quotient $PGO(q)$ de $GO(q)$ par le groupe k^* des homothéties de E . Ce groupe est ce qu'on peut appeler le groupe de la conique \bar{q} .

Soit $\Gamma = V(q)$ l'ensemble des zéros de q . On a vu que, dans le cas propre non vide, Γ détermine \bar{q} . Le groupe $PGL(E)$ opère aussi sur l'ensemble des parties de $\mathbf{P}(E)$ et, en particulier, sur les "coniques" $\Gamma = V(q)$. On peut donc aussi considérer le stabilisateur de Γ dans cette action. Dans le cas présent, ces deux groupes sont identiques :

3.2.1 Proposition. *Soit \bar{q} une conique propre non vide et $\Gamma = V(q)$ son ensemble de points. Les sous-groupes suivants de $PGL(E)$ sont identiques (et on les désignera dans ce qui suit comme le groupe de la conique Γ) :*

- 1) *le groupe $PGO(q)$, image du groupe des similitudes relatives à q ,*
 - 2) *le groupe $PO(q)$, image du groupe des isométries relatives à q ,*
 - 3) *le groupe des homographies \bar{u} qui conservent Γ : $\bar{u}(\Gamma) = \Gamma$.*
- De plus, tous ces groupes sont isomorphes au groupe $O^+(q)$ des isométries positives relatives à q .*

Démonstration. Il est clair que si \bar{u} est dans $PGO(q)$, \bar{u} conserve $V(q)$, cf. 2.2.1. Réciproquement, si on suppose qu'on a $\bar{u}(V(q)) = V(q)$ et si on pose $q' = q \circ u^{-1}$, on a $V(q') = V(q)$ et q' et q sont proportionnelles en vertu de 2.2.24.

Il est clair que $PO(q)$ est un sous-groupe de $PGO(q)$. Réciproquement, si u est dans $GO(q)$, on a $q \circ u = \lambda q$ avec $\lambda \in k^*$. Si A est la matrice de q et U celle de u , cela signifie qu'on a ${}^tUAU = \lambda A$. En prenant les déterminants, on a $(\det U)^2 \det A = \lambda^3 \det A$ (car E est de dimension 3). Cela montre que λ est un carré de k : $\lambda = \left(\frac{\det U}{\lambda} \right)^2$. Mais alors, si $\lambda = \alpha^2$, $\alpha^{-1}u$ est dans $O(q)$ et a même image que u dans le groupe projectif.

Enfin, l'isomorphisme entre $O^+(q)$ et $PO(q)$ résulte du fait que $-\text{Id}_E$ n'est pas dans $O^+(q)$, de sorte que $O(q)$ est réunion de $O^+(q)$ et $-O^+(q)$ qui ont même image dans $PGL(E)$.

3.2.2 L'isomorphisme avec $PGL(2, k)$

Dans ce paragraphe, nous donnons une autre raison de penser la conique comme une droite : leurs groupes d'automorphismes sont isomorphes.

3.2.2 Proposition. Soient $\Gamma = V(q)$ une conique propre non vide et $\bar{u} \in PO(q)$. La restriction de \bar{u} à Γ est une bijection de Γ qui conserve le birapport.

Démonstration. Soient a, b, c, d quatre points distincts de Γ et m un point quelconque de Γ . Par définition, on a $\llbracket a, b, c, d \rrbracket = \llbracket (ma), (mb), (mc), (md) \rrbracket$. Soient a', b', c', d', m' les images des points précédents par \bar{u} . Comme \bar{u} est dans $PO(q)$, ce sont des points de Γ . On sait, voir Partie I ??, que l'application induite par \bar{u} sur les droites de $\mathbf{P}(E)$ est une homographie de $\mathbf{P}(E^*)$ qui induit une homographie de la droite duale m^* sur $(m')^*$. Il en résulte qu'on a $\llbracket (ma), (mb), (mc), (md) \rrbracket = \llbracket (m'a'), (m'b'), (m'c'), (m'd') \rrbracket$, et, en vertu de 3.1.4, ce birapport est égal à $\llbracket a', b', c', d' \rrbracket$.

Nous pouvons maintenant prouver le résultat principal de ce paragraphe :

3.2.3 Théorème. L'application Φ qui à $\bar{u} \in PO(q)$ associe sa restriction $\bar{u}|_{\Gamma}$ induit un isomorphisme de $PO(q)$ sur le groupe $PGL(2, k)$ des homographies de la droite projective.

Démonstration. En vertu de 3.2.2, l'application Φ est un homomorphisme du groupe $PO(q)$ dans le groupe G des bijections de Γ qui conservent le birapport, groupe isomorphe à $PGL(2, k)$ en vertu de 3.1.5. Cet homomorphisme est injectif car la conique Γ contient au moins quatre points distincts, qui forment un repère, puisque trois ne sont pas alignés, de sorte que si \bar{u} est l'identité sur Γ c'est l'identité. Il est surjectif, car un élément de G est déterminé par l'image de trois points de Γ et qu'on a le lemme suivant :

3.2.4 Lemme. Le groupe $PO(q)$ est triplement transitif sur Γ .

Démonstration. Soient a, b, d (resp. a', b', d') trois points distincts de Γ . Il s'agit de montrer qu'il existe un élément de $PO(q)$ qui échange ces points. Soit c (resp. c') le point d'intersection des tangentes à Γ en a et b . En vertu de 2.2.24.1, a, b, c, d (resp. a', b', c', d') est un repère de $\mathbf{P}(E)$. Il existe donc une homographie \bar{u} qui envoie respectivement a, b, c, d sur a', b', c', d' . Mais, l'image de Γ par \bar{u} est une conique qui passe par a', b', d' et qui est tangente à $(c'a')$ et $(c'b')$ en a' et b' . En vertu de 2.2.24.2 l'unique conique qui vérifie ces propriétés est Γ . On a donc $\bar{u}(\Gamma) = \Gamma$ ce qui signifie que \bar{u} est dans $PO(q)$ et cela achève de montrer le lemme.

3.2.5 Remarque. Le théorème précédent montre qu'on peut, au choix, considérer les éléments du groupe $PO(q)$ d'une conique propre non vide, soit comme des bijections du plan, soit comme des bijections de la conique.

3.3 Les involutions d'une conique : points de Frégier

3.3.1 Le point de Frégier

Dans ce paragraphe nous déterminons les involutions de Γ . Nous désignons par ce mot les involutions de $PO(q)$, mais vues plutôt ici comme des bijections de $\Gamma = V(q)$. Ce sont donc, *via* le paramétrage, des involutions d'une droite projective. Nous allons donner une description géométrique très simple de ces involutions en utilisant les points du plan situés en dehors de la conique.

On commence par un lemme :

3.3.1 Lemme. *Soit Γ une conique propre non vide, $a, a'; b, b'; c, c'$ des points de Γ tels que a, a', b soient distincts. On suppose que les droites (aa') , (bb') et (cc') concourent en o (si b et b' coïncident, la droite (bb') est, comme à l'accoutumée, la tangente en b et de même pour (cc')). Alors on a l'égalité : $\llbracket a, a', b, c \rrbracket = \llbracket a, a', c', b' \rrbracket$.*

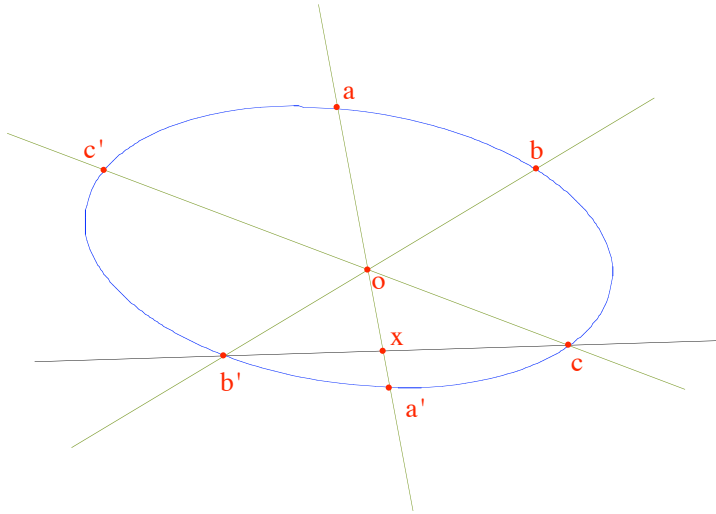


Figure 3.4: Preuve de 3.3.1

Démonstration. On appelle x le point d'intersection de (cb') et (aa') . On a les égalités de birapport $r := \llbracket a, a', b, c \rrbracket = \llbracket (b'a), (b'a'), (b'b), (b'c) \rrbracket$ (définition du birapport sur Γ), puis $r = \llbracket a, a', o, x \rrbracket$ (incidence sur (aa')), ensuite $r = \llbracket (ca), (ca'), (co), (cx) \rrbracket$ (incidence sur c^*), enfin $r = \llbracket a, a', c', b' \rrbracket$ (définition du birapport sur Γ).

3.3.2 Théorème-Définition. Soit Γ une conique propre non vide, o un point de $\mathbf{P}(E) - \Gamma$ et soit σ_o l'application de Γ dans elle-même définie comme suit :

- si m est un point de Γ tel que (om) est tangente à Γ , on pose $\sigma_o(m) = m$,
- sinon, la droite (om) recoupe Γ en un point m' et on pose $\sigma_o(m) = m'$.

Alors σ_o est une involution (homographique) de Γ . Le point o est appelé **point de Frégier** de l'involution σ_o , il est bien déterminé par l'involution et c'est un point fixe de celle-ci⁴. Tout point de la polaire de o est fixe par σ_o , toute droite passant par o est stable par σ_o . Le point o et les points de sa polaire sont les seuls points fixes de σ_o .

Toute involution de Γ est de cette forme.

Démonstration. On a vu, cf. 2.2.18, qu'il y a au plus deux tangentes à Γ issues de o et donc deux points de contact. Soit $a \in \Gamma$ un point distinct de ces points de contact. La droite (oa) recoupe donc Γ en $a' \neq a$ et σ_o échange a et a' . Soit $b \in \Gamma$ distinct de a, a' et soit $b' = \sigma_o(b)$. On sait que le groupe $PO(q)$ est le groupe des bijections de Γ qui conservent le birapport et qu'il est isomorphe à $PGL(2, k)$. Il existe donc une involution $j \in PO(q)$ définie par $j(a) = a'$, $j(a') = a$ et $j(b) = b'$. Nous allons montrer qu'on a $j = \sigma_o$. Pour cela, si c est un point quelconque de Γ , et si $c' = \sigma_o(c)$, il suffit de montrer que l'on a $\llbracket a, a', b, c \rrbracket = \llbracket a', a, b', c' \rrbracket$, mais c'est exactement 3.3.1 après double permutation.

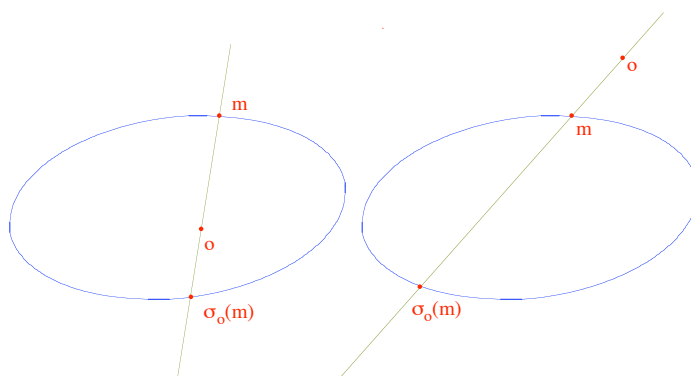


Figure 3.5: Involutions et points de Frégier

⁴La première apparition de ce point est due à Frégier, dans un article intitulé *Géométrie analytique. Théorèmes nouveaux, sur les lignes et surfaces du second ordre* et paru dans les Annales de Mathématiques pures et appliquées de 1816. Je cite le théorème originel pour montrer au lecteur que son sort aurait pu être pire. *Si deux lignes du second ordre, tracées sur un même plan, sont telles que le centre de la seconde soit situé sur le périmètre de la première ; toutes les cordes qui, dans celle-ci, se termineront à ses intersections avec les prolongemens de deux diamètres conjugués de l'autre, se couperont en un même point, situé sur le conjugué du diamètre qui, dans la seconde courbe, est tangent à la première.*

Cette preuve montre aussi que toute involution j est de la forme σ_o . Pour une preuve algébrique, voir 3.3.8.

Si la droite (om) est tangente à Γ en m , comme m est fixe par σ_o , (om) est invariante. Il en est de même pour une droite passant par o qui coupe Γ en deux points. Toutes les droites passant par o et coupant Γ sont donc stables par σ_o . Comme Γ a au moins quatre points, dont trois ne sont jamais alignés, il y a au moins deux telles droites distinctes et il en résulte que o est fixe par σ_o .

La polaire Ω de o est alors invariante par σ_o . Si le corps k a au moins cinq éléments⁵ il y a au moins trois droites issues de o qui coupent Γ . Ces droites rencontrent Ω en trois points qui sont fixes par σ_o , de sorte que Ω est fixe par σ_o . Si maintenant D est une droite quelconque passant par o (ne rencontrant pas nécessairement Γ), elle coupe Ω en un point m . Comme o et m sont fixes par σ_o , la droite D est stable.

Enfin, si d est un point distinct de o et non situé sur Ω , il ne peut être fixe (sinon, en prenant deux points de Ω non alignés avec o et d , on voit que σ_o fixerait un repère du plan).

3.3.2 Le théorème de Cartan-Dieudonné

Il s'agit du théorème algébrique bien connu sur la génération du groupe orthogonal par des involutions, cf. par exemple [Per96]. Dans le cas présent, il devient :

3.3.3 Théorème. *Soit $f \in PO(q)$. Alors f est produit d'au plus deux involutions.*

Démonstration. Vu l'isomorphisme de $PO(q)$ et de $PGL(2, k)$ (cf. 3.2.3), cela résulte de Partie I, ?? mais la remarque ci-dessus donne une preuve géométrique directe.

3.3.4 Remarques.

1) On peut démontrer directement le résultat précédent et ainsi réaliser pratiquement la décomposition d'une homographie f en produit $f = i_v \circ i_u$ de deux involutions de points de Frégier v, u . Si l'on se donne f par trois points a, b, c et leurs images a', b', c' , il suffit de prendre, par exemple, u à l'intersection de (ab') et (ba') et v est alors déterminé comme intersection de $(a'b')$ et $(c'i_u(c))$, voir fig. 3.6. Le lecteur vérifiera que la construction fonctionne même si certains des points sont confondus, à condition de remplacer sécante par tangente.

⁵Le lecteur vérifiera que la propriété est encore vraie dans le seul cas douteux : si le corps k est égal à \mathbf{F}_3 et si les 4 points de la conique sont sur deux droites issues de o .

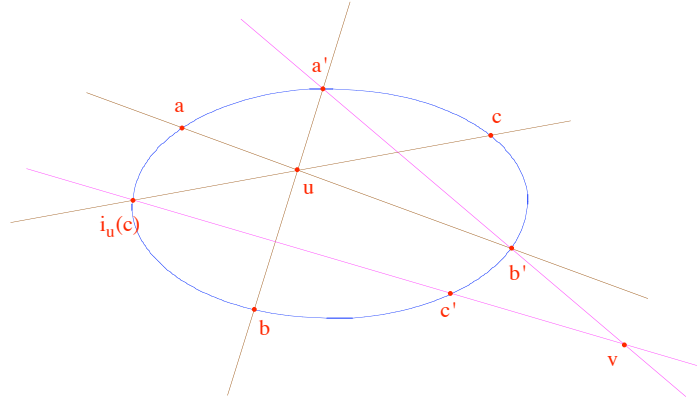


Figure 3.6: Décomposition d'une homographie en produit de deux involutions.

2) Il sera utile (cf. 3.3.10) de noter qu'on peut écrire tout élément de $PO(q)$ comme produit de deux involutions exactement. C'est évident en ce qui concerne l'identité. Si i est une involution de point de Frégier a la construction précédente montre qu'elle se décompose en le produit de deux involutions de points de Frégier b, c et que le triangle abc est alors autopolaire, voir aussi 3.3.9 ou exercice 3.6.3.

3.3.3 Axe d'homographie

La proposition suivante est essentielle pour mener les constructions géométriques liées aux homographies :

3.3.5 Proposition. *Soit $f \in PO(q)$, $f \neq \text{Id}$. Il existe une unique droite D de $\mathbf{P}(E)$ telle que, pour tous $a, b \in \Gamma$, avec $a \neq b$ on ait, en posant $a' = f(a)$:*

$$b' = f(b) \iff (a'b) \cap (ab') \subset D$$

(en convenant que si, par exemple, les points a' et b coïncident, la droite $(a'b)$ est la tangente à Γ en a'). La droite D s'appelle **l'axe** de f , elle est invariante par f . Les points fixes de f sur Γ sont les points de $\Gamma \cap D$. Le pôle de D est un point fixe de f .

Si f est une involution de point de Frégier u , l'axe de f est la polaire de u ; si f est produit de deux involutions de points de Frégier u, v , l'axe de f est la droite (uv) .

Démonstration. Vu le théorème de Cartan-Dieudonné il suffit de montrer l'existence et l'unicité de l'axe lorsque f est une involution ou un produit de deux involutions.

1) Si f est l'involution de point de Frégier u , le fait que $(a'b)$ et (ab') se coupent sur la polaire de u résulte de la construction de celle-ci, cf. 2.3.11. Cela montre l'existence et l'unicité de l'axe dans ce cas. Le point de Frégier étant un point fixe de f , sa polaire est bien invariante.

2) Si $f = j \circ i$ est produit de deux involutions de points de Frégier v, u distincts, on pose $a'' = i(a)$, $b'' = i(b)$. On a alors $a' = j(a'') = f(a)$, $b' = j(b'') = f(b)$. On sait que u est l'intersection de (aa'') et (bb'') et v celle de $(a'a'')$ et $(b'b'')$ et il s'agit de montrer que (ab') et (ba') se coupent sur (uv) : c'est le théorème de Pascal appliqué à a, a', b'' et b, b', a'' ! Là encore, on a prouvé ainsi l'existence et l'unicité de l'axe. Comme u et v sont fixés respectivement par i et j , la droite (uv) est invariante par f et son pôle est fixe.

La définition de l'axe (ou sa caractérisation en termes de la décomposition de f) montre que les points de $D \cap \Gamma$ sont fixes.

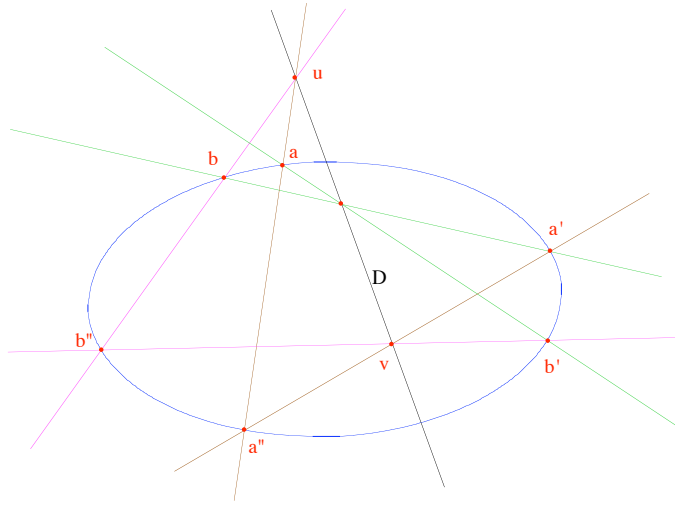


Figure 3.7: L'axe d'homographie dans le cas du produit de deux involutions.

3.3.6 Remarques.

1) La proposition précédente donne un moyen de construire l'image d'un point de Γ par f lorsqu'on connaît l'axe de f et l'image a' d'un point particulier a : on obtient l'image b' de b en utilisant le fait que (ab') et $(a'b)$ se coupent sur l'axe.

2) Toute droite D du plan est axe d'une homographie : il suffit de prendre le produit de deux involutions de points de Frégier situés sur D .

3.3.4 Application : le problème de Castillon

Le problème est le suivant : on suppose donnés une conique propre non vide Γ et n points a_1, \dots, a_n du plan, non sur Γ . Il s'agit de trouver des points $b_1, \dots, b_n \in \Gamma$ tels que pour tout k , $a_k \in (b_k b_{k+1})$ (les indices sont pris modulo n et on maintient la convention habituelle si les points coïncident). Supposons le problème résolu et considérons, pour tout k , l'involution σ_k de point de Frégier a_k qui échange b_k et b_{k+1} . Alors, l'homographie $f = \sigma_n \circ \dots \circ \sigma_1$ fixe b_1 . Le point b_1 est donc sur l'axe de f que l'on obtient en construisant les images par f de trois points u, v, w de Γ , cf. fig. 3.8 avec $n = 3$. Si le corps de base est \mathbf{R} , il peut y avoir 0, 1 ou 2 solutions.

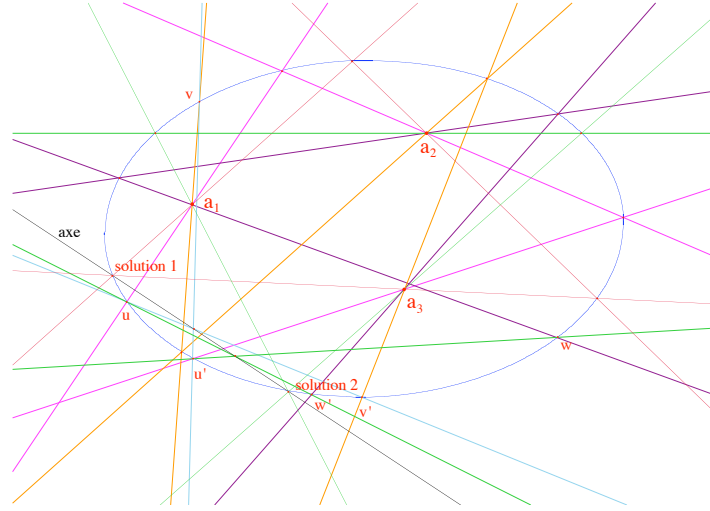


Figure 3.8: Le problème de Castillon.

3.3.5 Applications de Frégier à l'étude des groupes

L'objectif de ce paragraphe est de montrer que la géométrie peut permettre de retrouver des résultats sur la structure des groupes : sous-groupes distingués, automorphismes (voir exercice 3.6.11), etc.

Dans tout ce paragraphe q est une forme quadratique non dégénérée sur un espace vectoriel E de dimension 3.

Retour sur les involutions

Nous faisons d'abord le lien entre les involutions du groupe $O(q)$ et celles de $PO(q)$. Les premiers résultats sont valables pour une forme q non

dégénérée, même si $V(q)$ est vide. Le premier lemme montre qu'il n'y a pas d'involutions nouvelles dans $PO(q)$:

3.3.7 Lemme. *Soit $u \in O(q)$. On suppose que \bar{u} est une involution de $PO(q)$. Alors u est une involution.*

Démonstration. Dire que \bar{u} est une involution signifie qu'on a $u^2 = \lambda \text{Id}$ dans E . Comme u^2 est une isométrie, cela impose $\lambda = \pm 1$ (cf. 1.3.2.4). Mais on a aussi $\det u^2 = (\det u)^2 = 1 = \lambda^3$ et cela impose $\lambda = 1$.

Il reste à voir ce que deviennent les involutions de $O(q)$ en projectif. Rappelons, cf. 1.3.5, que le groupe $O(q)$ contient *a priori* trois types d'involutions : $-\text{Id}_E$, qui donne l'identité dans $\mathbf{P}(E)$, les réflexions (symétries orthogonales par rapport à un plan) et les renversements ou demi-tours (symétries orthogonales par rapport à une droite). Mais, si τ_H est la réflexion par rapport au plan H et σ_D le renversement d'axe $D = H^\perp$, on a $\tau_H = -\sigma_D$, de sorte que ces éléments sont égaux dans $PO(q)$. On peut donc se limiter aux renversements dans l'étude des involutions de $PO(q)$. On a alors le résultat suivant :

3.3.8 Proposition. *On suppose que $V(q)$ est non vide. Soit $\sigma_D \in O(q)$ le renversement d'axe la droite vectorielle D . Alors, l'involution $\bar{\sigma}_D$ a pour point de Frégier le point $d = p(D)$ et pour axe la droite $p(D^\perp)$.*

Démonstration. Il suffit de prouver la première assertion. Or, si x est un vecteur isotrope, le vecteur $x + \sigma_D(x)$ est invariant par σ_D , donc est dans D . Projectivement, cela signifie exactement que \bar{x} , $\overline{\sigma_D(x)}$ et d sont alignés. Appliquant cela à deux paires de vecteurs isotropes échangés par σ_D , on voit que d est le point de Frégier de $\bar{\sigma}_D$.

3.3.9 Remarques.

- 1) Si on convient de noter encore d un vecteur non nul de D , une autre preuve du résultat précédent consiste à utiliser la formule $\sigma_D(x) = x - 2 \frac{\varphi(d, x)}{q(d)} d$ qui montre que les points $m = p(x)$, $\sigma_D(m)$ et d sont alignés.
- 2) Avec la proposition, le fait qu'une involution de $PO(q)$ est aussi produit de deux involutions (cf. 3.3.4) devient évident. En effet, si on a un renversement d'axe $D = (e_1)$ et si on complète e_1 en une base orthogonale e_1, e_2, e_3 , il est clair sur les matrices que σ_D est le produit des deux renversements d'axes e_2, e_3 .

La norme spinorielle

Dans ce paragraphe nous allons retrouver un résultat algébrique concernant la structure du groupe $PO(q) = O^+(q)$. Pour des preuves algébriques, cf. [Die70], [Art62] ou [Per96].

3.3.10 Proposition. *On suppose que $V(q)$ est non vide (i.e. que q est d'indice ≥ 1). Soit $u \in PO(q)$. On écrit u comme produit de deux involutions de points de Frégier a et b (cf. ci-dessus 3.3.9). Alors l'image de $q(a)q(b)$ dans k^*/k^{*2} ne dépend que de u et pas du choix des involutions. L'application $\theta : PO(q) \rightarrow k^*/k^{*2}$ qui à u associe $\overline{q(a)q(b)}$ est un homomorphisme de groupes, surjectif. Le noyau de θ est le groupe des commutateurs $\Omega(q)$ de $O^+(q) \simeq PO(q)$. Il est isomorphe à $PSL(2, k)$.*

Démonstration. Nous allons prouver que $q(a)q(b)$, dans k^*/k^{*2} , n'est autre que le déterminant de $\Phi(u)$, où $\Phi : PO(q) \rightarrow PGL(2, k)$ est l'isomorphisme vu en 3.2.3. Pour cela nous montrons le lemme suivant :

3.3.11 Lemme. *Soit Γ une conique propre non vide d'équation $q = Y^2 - XT$, soit $a \notin \Gamma$ et $\sigma_a \in PO(q)$ l'involution de point de Frégier a . Avec les notations de 3.2.3, on a la formule $\det(\Phi(\sigma_a)) = -\overline{q(a)}$ dans k^*/k^{*2} .*

Démonstration. (du lemme) On pose $a = (\alpha, \beta, \gamma)$. La conique est paramétrée par $(\lambda^2, \lambda\mu, \mu^2)$. On part d'un point $x \in \Gamma$ de paramètre (λ, μ) et on effectue σ_a . On considère d'abord la droite (ax) . Son équation est $uX + vY + wT$ avec :

$$u = \beta\mu^2 - \gamma\lambda\mu, \quad v = \gamma\lambda^2 - \alpha\mu^2, \quad w = \alpha\lambda\mu - \beta\lambda^2.$$

On cherche les points d'intersection de cette droite avec Γ comme des points de paramètres (p, q) donnés par l'équation :

$$(\beta\mu^2 - \gamma\lambda\mu)p^2 + (\gamma\lambda^2 - \alpha\mu^2)pq + (\alpha\lambda\mu - \beta\lambda^2)q^2 = 0.$$

On obtient, outre le point initial x de paramètre (λ, μ) , le point de paramètre $(-\beta\lambda + \alpha\mu, -\gamma\lambda + \beta\mu)$. On en déduit que $\Phi(\sigma_a)$ est l'involution de matrice

$$\begin{pmatrix} -\beta & \alpha \\ -\gamma & \beta \end{pmatrix}, \text{ et de déterminant } -\beta^2 + \alpha\gamma = -q(a) \text{ comme annoncé.}$$

Les assertions sur la surjectivité de θ ou le fait que $\Omega(q)$ soit le groupe des commutateurs de $O^+(q)$ résultent alors des assertions analogues sur $PGL(2, k)$ et sont bien connues dans ce cas, cf. par exemple [Per96] Ch. IV.

3.3.12 Corollaire. *On suppose que $\Delta(q)$ est l'opposé d'un carré, cf. 2.1.5. Si a est un point de $\mathbf{P}(E) - \Gamma$ et σ_a l'involution de point de Frégier a , on a $\theta(\sigma_a) = -q(a)$ dans k^*/k^{*2} . L'involution σ_a est dans $\Omega(q)$ si et seulement si $q(a)$ est l'opposé d'un carré.*

Démonstration. On complète a en une base orthogonale a, b, c . On a $\sigma_a = \sigma_b \sigma_c$ (cf. 3.3.9), de sorte que la norme spinorielle de σ_a est l'image de $q(b)q(c)$ dans k^*/k^{*2} (cf. 3.3.10). Mais comme $\Delta(q) = q(a)q(b)q(c)$, on a $-q(a) = q(b)q(c)$ dans k^*/k^{*2} .

Le cas de \mathbf{R}

Dans ce paragraphe on suppose $k = \mathbf{R}$ et on considère une conique propre Γ non vide d'équation q , avec $\Delta(q) = -1$ dans k^*/k^{*2} (par exemple $q = Y^2 - XT$ ou $q = X^2 + Y^2 - T^2$). On rappelle (cf. 2.2.19) que le complémentaire $\mathbf{P}(E) - \Gamma$ est réunion de deux composantes connexes : l'intérieur \mathbf{K} défini par $q < 0$ et l'extérieur \mathbf{T} défini par $q > 0$. Le corollaire précédent devient :

3.3.13 Corollaire. *Si a est un point de $\mathbf{P}(E) - \Gamma$ et σ_a l'involution de point de Frégier a , on a $\theta(\sigma_a) = 1$ (resp. -1) dans k^*/k^{*2} si a est dans \mathbf{K} (resp. dans \mathbf{T}).*

3.3.14 Remarque. Si on choisit de prendre une forme q de discriminant $+1$ il y a des variations de signes dans ce qui précède, mais le point essentiel demeure : l'intérieur de la conique garde un sens (c'est la partie qui ne contient pas de droites) et les involutions de norme spinorielle positive sont celles dont les points de Frégier sont intérieurs.

3.3.6 Retour sur les homographies d'une droite sur une autre

Nous avons fait dans la Partie I un usage intensif des perspectives, vues comme homographies d'une droite sur une autre. Pour les homographies qui ne sont pas des perspectives, la définition du birapport sur une conique permet de donner une représentation commode et efficace.

L'homographie associée à deux tangentes à une conique

3.3.15 Proposition. *Soit Γ une conique propre non vide et soient D, D' deux droites, tangentes à Γ respectivement en des points p et p' distincts, et se coupant en e . On considère l'application $f : D \rightarrow D'$ définie comme suit :*

- *si $m \in D$ est distinct de p et e , on lui associe le point d'intersection de D' et de la deuxième tangente à Γ passant par m ,*
- *si m est en p on lui associe le point e ,*
- *si m est en e on lui associe p' .*

Alors, l'application f est une homographie que l'on notera $f_{D,D',\Gamma}$.

Démonstration. On peut montrer cette proposition par le calcul en utilisant un repère adapté comme en 2.2.24. On peut aussi procéder directement. L'application polaire $m \mapsto m^\perp := \Delta$ de $\mathbf{P}(E)$ dans $\mathbf{P}(E^*)$ est une homographie en vertu de 2.3.5. On la restreint à D et on obtient une homographie de D sur p^* . Dans cette homographie, le point p donne D et le point e donne (pp') . On considère ensuite l'application de p^* sur Γ qui associe à Δ le point d'intersection q de Δ et Γ distinct de p (sauf si Δ est égale à D auquel cas on lui associe p). On note que l'image de (pp') est p' . Cette transformation conserve le birapport, par définition du birapport sur la conique. On associe ensuite au point q de Γ sa tangente $q^\perp = (mq)$. Cette application conserve le birapport en vertu de 3.1.8 et son image est Γ^* , conique duale de Γ , le point p donnant D et le point p' , D' . Enfin, on associe à une tangente T son point d'intersection avec D' (ou p' si $T = D'$). Par définition du birapport de quatre tangentes, cf. 3.1.7, cette application conserve le birapport. La composée de toutes ces applications n'est autre que f et, comme elle conserve le birapport, c'est bien une homographie.

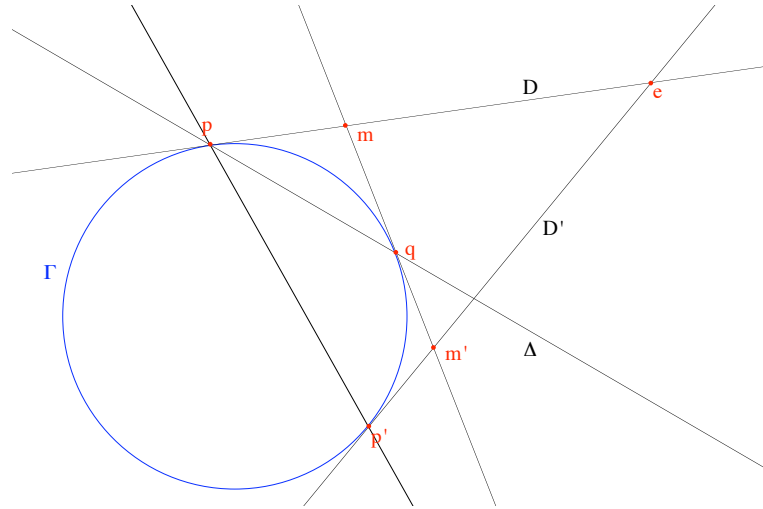


Figure 3.9: L'homographie associée à deux tangentes.

Toutes les homographies sont (presque) de ce type

Nous allons montrer que toutes les homographies sont soit des perspectives, soit du type précédent. Pour cela nous aurons besoin d'un lemme⁶ :

⁶Il s'agit de montrer qu'une conique est déterminée par cinq conditions, cf. 4.1.3.

3.3.16 Lemme. Soient D, D' deux droites distinctes se coupant en e , soient $p, a \in D$ et $p', a' \in D'$ des points distincts et distincts de e . Il existe une unique conique Γ propre qui est tangente à D en p , à D' en p' et à (aa') .

Démonstration. On peut supposer $p = (1, 0, 0)$, $p' = (0, 1, 0)$, $e = (0, 0, 1)$, donc D et D' d'équations $Y = 0$ et $X = 0$ respectivement. La droite (aa') admet alors pour équation $uX + vY + wT = 0$ avec u, v, w non nuls et on vérifie que l'unique conique convenable a pour équation $4uvXY - w^2T^2 = 0$.

3.3.17 Proposition. Soient D, D' deux droites distinctes de $\mathbf{P}(E)$ et soit $f : D \rightarrow D'$ une homographie. Alors f est soit une perspective, soit une application $f_{D,D',\Gamma}$ du type précédent.

Démonstration. Supposons que f n'est pas une perspective. On appelle e le point d'intersection de D et D' . On a donc $f(e) \neq e$ (voir Partie I Exercice ??) et on pose $f(e) = p'$ et $f^{-1}(e) = p$. Soit $a \in D$ distinct de e et p et posons $a' = f(a)$ (a' est distinct de e et p'). En vertu du lemme, il existe une conique propre Γ tangente à D en p , à D' en p' et à (aa') . L'homographie $f_{D,D',\Gamma}$ coïncide avec f en e, p, a donc elle lui est égale.

3.3.7 Une application : le théorème de Newton

Nous revenons dans ce paragraphe sur le théorème de Newton, déjà abordé dans les Parties I et II, mais traité ici par une méthode proche de celle utilisée par Newton lui-même⁷.

Préliminaire : le lemme XXIII de Newton

Il s'agit d'un lemme préliminaire au théorème sur les milieux des côtés d'un quadrilatère complet (voir Partie I ??). La forme originelle de ce résultat (que le lecteur prouvera sans peine avec des techniques de géométrie affine) est la suivante :

3.3.18 Théorème. Soient D, D' deux droites distinctes du plan affine, et soient $a, b, c \in D$, $a', b', c' \in D'$. On suppose qu'on a la relation $\frac{\overline{a'c'}}{\overline{ac}} = \frac{\overline{a'b'}}{\overline{ab}}$. Alors, les milieux i, j, k de $[aa']$, $[bb']$, $[cc']$ sont alignés.

En notant que l'hypothèse du théorème 3.3.18 équivaut à l'existence d'une application affine de D sur D' qui envoie a, b, c sur a', b', c' , on voit que ce

⁷Dans toute cette partie de son œuvre, Newton s'intéresse en priorité aux coniques (vues comme trajectoires des planètes), et notamment à leurs tangentes.

résultat est conséquence de sa variante projective (prendre (dd') comme droite à l'infini et $r = -1$) :

3.3.19 Théorème. (Le lemme XXIII) Soient D, D' deux droites distinctes du plan projectif, soit $f : D \rightarrow D'$ une homographie et soient $a, b, c, d \in D$ et $a', b', c', d' \in D'$ leurs images par f . On appelle α, β, γ les intersections respectives de (aa') , (bb') , (cc') avec (dd') et on considère les points i, j, k de (aa') , (bb') et (cc') vérifiant $\llbracket a, a', \alpha, i \rrbracket = \llbracket b, b', \beta, j \rrbracket = \llbracket c, c', \gamma, k \rrbracket = r$, où r est un élément de $\mathbf{P}^1(k)$ donné. Alors, les points i, j, k sont alignés.

Démonstration. On utilise le lemme suivant :

3.3.20 Lemme. Soit Γ une conique propre non vide et soient D, D' deux tangentes distinctes à Γ . On considère l'homographie $f = f_{D, D', \Gamma} : D \rightarrow D'$, voir 3.3.15. Soit d un point fixe de D et d' son image par f . Soit m un point variable de D d'image m' et soit $r \in \mathbf{P}^1(k)$. On note μ le point d'intersection de (mm') et (dd') et Δ la tangente à Γ définie par $\llbracket D, D', (dd'), \Delta \rrbracket = r$. Alors, le lieu, quand m varie sur D , du point i de (mm') défini par $\llbracket m, m', \mu, i \rrbracket = r$ est la droite Δ .

Démonstration. C'est exactement la définition du birapport de quatre tangentes à une conique.

On peut alors finir la preuve de 3.3.19. Si f est une perspective, les points α, β, γ sont confondus et i, j, k sont alignés sur (ei) où e désigne le point d'intersection de D et D' . Sinon, en vertu de 3.3.17, on est dans le cas d'application du lemme 3.3.20, qui donne le résultat escompté.

Le théorème de Newton

Rappelons la variante projective de ce théorème (voir Partie I ??) :

3.3.21 Théorème. Soit a, b, c, d un repère de $\mathbf{P}(E)$ et soient e et f les intersections de (ab) , (cd) et (ad) , (bc) respectivement. Soit Ω une droite et p, q, r les intersections de Ω avec (ca) , (bd) et (ef) . On appelle i, j, k les conjugués harmoniques de p, q, r par rapport à c, a ; b, d et e, f . Alors i, j, k sont alignés.

La variante affine usuelle s'obtient en prenant pour Ω la droite de l'infini. En notant que les points a, b, c, d, e, f jouent le même rôle, on voit que le théorème résulte du suivant :

3.3.22 Théorème. Soit a, b, c, d un repère de $\mathbf{P}(E)$ et soit Γ une conique propre tangente⁸ à (ab) , (bc) , (cd) , (da) . Soient Ω une droite et o le pôle de

⁸Le lecteur montrera qu'il en existe par une méthode analogue à celle de 3.3.20 ou il patientera jusqu'à 4.1.3.

Ω par rapport à Γ . On appelle p et q les intersections de (ac) et (bd) avec Ω et i, j les conjugués harmoniques de p, q par rapport à c, a et b, d . Alors, o, i, j sont alignés.

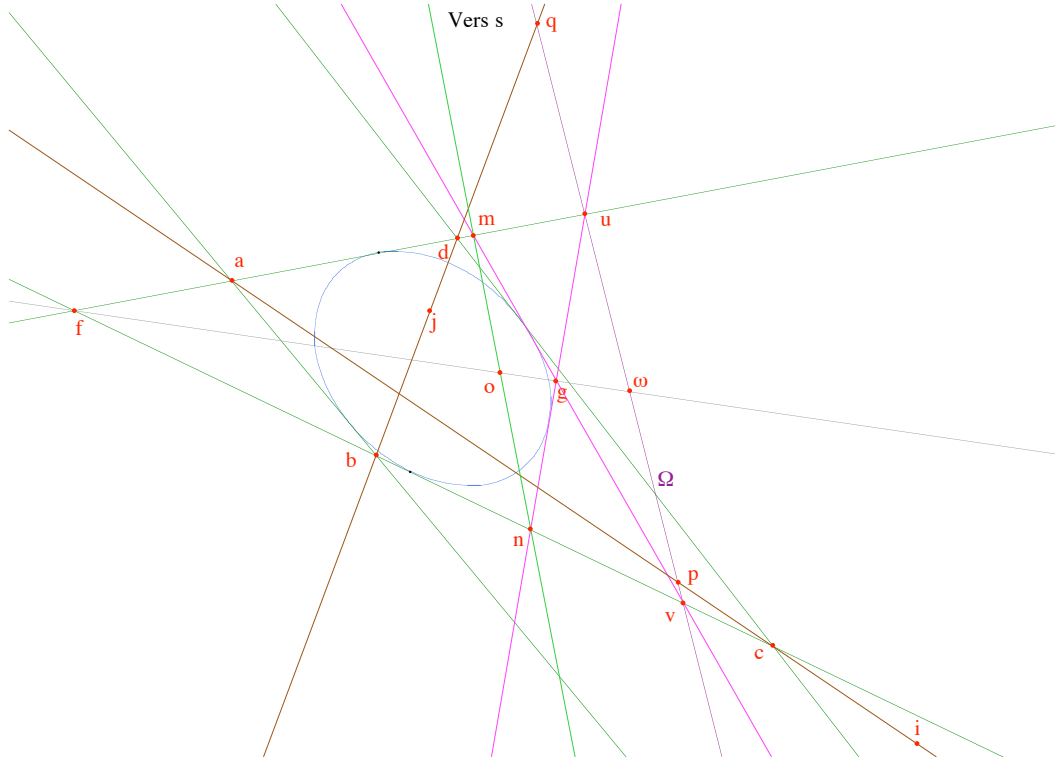


Figure 3.10: Variante du théorème de Newton

Démonstration. On note f l'intersection de (ad) et (bc) , ω l'intersection de Ω et (of) et g le point défini par $\llbracket o, \omega, f, g \rrbracket = -1$. Soit u (resp. v) l'intersection de Ω et de (ad) (resp. (bc)) et soit m (resp. n) le point d'intersection de (ad) et (gv) (resp. (bc) et (gu)). On a le lemme suivant :

3.3.23 Lemme. *Les droites (gu) et (gv) sont tangentes à Γ .*

Démonstration. (du lemme) On considère l'involution τ de point de Frégier o et d'axe Ω , vue comme une involution du plan tout entier. Elle laisse stable Γ et fixe o et les points de Ω . En particulier, on a $\tau(u) = u$. La droite (ωu) est stable par τ et, comme on a $\llbracket o, \omega, f, g \rrbracket = -1$, on a $\tau(f) = g$. Comme (fu) est tangente à Γ , il en est de même de $\tau((fu)) = (gu)$. Le raisonnement est identique pour (gv) .

On notera que τ échange aussi m et n (car on a $m = (fu) \cap (gv)$ et $n = (gu) \cap (fv)$), ce qui montre qu'ils sont alignés avec o (car les droites passant par o sont stables par τ) et que, si s est l'intersection de Ω et de (mn) , on a $\llbracket m, n, o, s \rrbracket = -1$.

Revenons à 3.3.22. On considère d'abord l'homographie $\varphi = f_{(ad),(bc),\Gamma}$ associée aux tangentes à Γ . On a donc $\varphi(d) = c$, $\varphi(a) = b$ et, en vertu du lemme, $\varphi(u) = n$ et $\varphi(m) = v$.

On considère ensuite l'involution σ de (bc) qui échange b et c et envoie v sur n . Elle envoie aussi n sur v . La composée $\sigma\varphi$ envoie a sur c , d sur b , m sur n et u sur v . On conclut en utilisant le lemme XXIII appliqué à la droite $(uv) = \Omega$. Elle coupe respectivement (ac) en p , (bd) en q et (mn) en s . Les conjugués harmoniques de ces points par rapport à a, c ; b, d et m, n étant respectivement i, j, o , on a le résultat.

3.4 Autour d'un théorème de Poncelet

Dans cette section, nous montrons un théorème de Poncelet (qu'on peut voir comme un résultat préliminaire à son grand théorème sur les polygones inscrits et circonscrits aux coniques que nous verrons au chapitre suivant, voir 4.5.4). Ce qui nous a paru digne d'intérêt n'est pas tant le résultat, somme toute anecdotique, mais plutôt la méthode utilisée, qui met en œuvre deux des outils favoris de Poncelet :

- l'utilisation systématique de la projection (ou, ce qui revient au même, de résultats de transitivité des homographies) pour ramener le problème à un cas particulier (ici celui d'un cercle),
- le passage par les nombres complexes.

Nous verrons aussi dans le dernier paragraphe une preuve algébrique plutôt plus simple que celle de Poncelet.

Dans toute cette section on suppose $k = \mathbf{R}$.

3.4.1 L'énoncé

Le résultat suivant, que nous désignerons ci-dessous comme *lemme de Poncelet*, est en substance dans le *Traité des propriétés projectives* p. 143 :

3.4.1 Proposition. *Soit Γ une conique propre et soient a, b deux points distincts du plan non situés sur Γ . On suppose que a et b ne sont pas conjugués par rapport à Γ . Soit p un point de Γ . Les droites (ap) et (bp) recoupent respectivement Γ en c et d . Les tangentes à Γ en c et d se coupent en m . Alors, le point m décrit une conique C .*

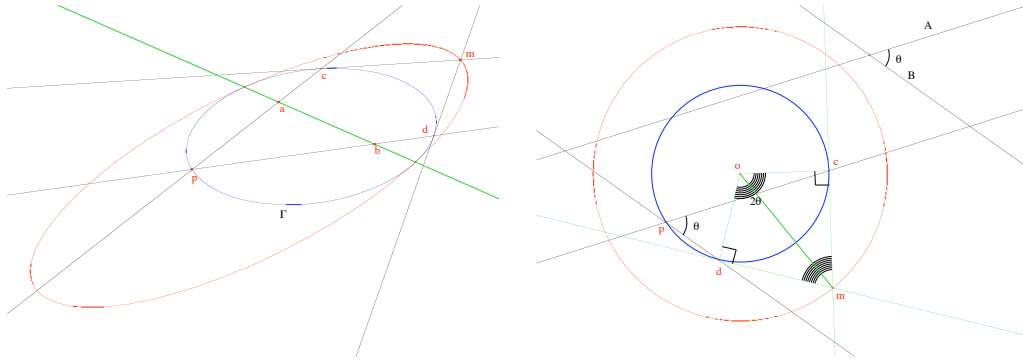


Figure 3.11: Le lemme de Poncelet, cas d'une ellipse, cas du cercle

Dans ce qui suit nous ne prouverons ce résultat qu'avec l'hypothèse supplémentaire que la droite (ab) n'est pas tangente à Γ . En revanche, la démonstration qui utilise 3.4.20 s'applique dans tous les cas, voir 3.4.22.

3.4.2 Remarques. 1) La construction donnée ci-dessus ne s'applique pas lorsque p est un point d'intersection de Γ et de la droite (ab) . En effet, si q est le second point d'intersection de (ab) et de Γ , on a alors $c = d = q$ et les tangentes en c, d sont égales. Dans ce cas, on convient que le point m est le point q et on verra en 3.4.18 que les coniques C et Γ sont bitangentes en p et q .

2) Dans le cas où a et b sont conjugués, on montre que m décrit (ab) . Voir 3.4.22 ou exercice 3.6.12.

3.4.2 Le cas d'un cercle et de deux points à l'infini

On commence par prouver :

3.4.3 Proposition. Soit Γ un cercle du plan affine euclidien, de centre o et de rayon R , et soient A, B deux droites ni parallèles ni perpendiculaires. Soit p un point de Γ . Les parallèles à A et B passant par p recoupent respectivement Γ en c et d . Les tangentes à Γ en c et d se coupent en m . Alors, le point m décrit un cercle de même centre que Γ .

Démonstration. Appelons θ l'angle aigu formé par les droites A, B . Le théorème de l'angle inscrit montre que l'angle au centre \widehat{cod} est égal à 2θ et, comme les tangentes sont symétriques par rapport à (om) , on a $\widehat{com} = \theta$. Comme le triangle com est rectangle en c , la distance $om = \frac{R}{\cos \theta} = R'$ est constante, ce qui montre que m décrit le cercle de centre o et de rayon R' .

3.4.4 Remarque. Si les droites A, B sont perpendiculaires, les tangentes en c et d sont parallèles et m décrit la droite de l'infini.

3.4.3 Les résultats de transitivité

Ce que dit Poncelet

La transitivité est au cœur de la méthode de Poncelet. Il montre notamment, en utilisant systématiquement les projections, qu'on peut transformer toute conique en un cercle. Voilà ce qu'il dit exactement :

Une figure étant donnée, si l'on veut rechercher quelles sont les propriétés de position dont elle jouit, on examinera si elle peut être projetée suivant une figure plus simple ; si cela a lieu, on cessera de s'occuper de la première figure et on recherchera seulement, sur sa projection plus simple, les propriétés que l'on avait particulièrement en vue ; car d'après ce qui précède, ces propriétés appartiendront aussi à la figure considérée d'abord.

Dans ce qui suit, et conformément aux principes énoncés dès l'introduction, nous utiliserons les homographies du plan (et non les projections centrales comme Poncelet) pour passer d'une conique à une autre. Cependant, il faut comprendre que cela revient exactement au même puisque les projections centrales (ou perspectives) sont des homographies (voir Partie I exercice ??) et que toute homographie est composée de telles projections.

Avec les outils algébriques

Dans ce paragraphe, le corps k est quelconque.

3.4.5 Proposition.

- 1) Soient Γ, Γ' deux coniques propres non vides. Il existe $u \in PGL(E)$ telle que $u(\Gamma) = \Gamma'$.
- 2) Soient Γ, Γ' deux coniques propres non vides et a, b, c (resp. a', b', c') des points distincts de Γ (resp. Γ'). Il existe $u \in PGL(E)$ telle que $u(\Gamma) = \Gamma'$ et $u(a) = a', u(b) = b', u(c) = c'$.
- 3) Soient Γ, Γ' deux coniques propres non vides d'équations respectives q, q' et soient a, a' des points de $\mathbf{P}(E)$ n'appartenant pas à Γ et Γ' respectivement. Il existe $u \in PGL(E)$ vérifiant $u(\Gamma) = \Gamma'$ et $u(a) = a'$ si et seulement si⁹ on a $\Delta(q)q(a) = \Delta(q')q'(a')$ dans k^*/k^{*2} . Si le corps k est algébriquement clos il n'y a pas de condition sur a, a' ; si k est le corps des réels la condition est que les points soient dans la même position par rapport à Γ et Γ' (i.e. tous

⁹Si l'on veut éviter la présence du discriminant, on peut imposer à toutes les formes de vérifier $\Delta(q) = -1$ modulo les carrés.

deux intérieurs ou tous deux extérieurs).

4) Soient Γ, Γ' deux coniques propres non vides d'équations respectives q, q' et soient D, D' des droites de $\mathbf{P}(E)$ non tangentes à Γ et Γ' respectivement. Il existe $u \in PGL(E)$ vérifiant $u(\Gamma) = \Gamma'$ et $u(D) = D'$ si et seulement si on a $\Delta(q^*)q^*(D) = \Delta(q'^*)q'^*(D')$ dans k^*/k^{*2} . Si le corps k est algébriquement clos il n'y a pas de condition sur D, D' ; si k est le corps des réels la condition est que les droites soient dans la même position par rapport à Γ et Γ' (i.e. toutes deux sécantes ou toutes deux extérieures).

Démonstration. Le premier point a été vu en 2.2.26. Le second résulte du premier et de 3.2.4 appliqué à Γ' . Les autres seront démontrés dans la Partie IV en utilisant le théorème de Witt pour le cas d'un corps quelconque. Pour le cas de \mathbf{R} , voir ci-dessous.

3.4.6 Remarque. Attention, une condition aussi innocente en apparence que le fait que D rencontre Γ en deux points implique que $q^*(D)$ est un carré (si l'on suppose $\Delta(q) = -1$), voir exercice 2.4.1. En particulier, il y a nombre de droites sécantes sur \mathbf{R} qui ne le sont pas sur \mathbf{Q} , par exemple la droite $Y = X$ et la conique $X^2 + Y^2 - T^2 = 0$.

Le cas réel par des voies géométriques

Il s'agit de montrer les points 3 et 4 de 3.4.5 dans le cas réel. Par dualité on peut se contenter de prouver le point 3.

Le cas où les points sont extérieurs est facile en prenant un repère adapté comme en 2.2.24. Il reste le cas où les points sont intérieurs. On commence par envoyer Γ sur Γ' et on est ramené à prouver :

3.4.7 Lemme. Soit Γ une conique d'équation q , a, b des points intérieurs. Il existe $u \in PO(q)$ telle que $u(a) = b$.

Démonstration. On cherche u comme une involution de point de Frégier m . Pour cela on considère le pôle c de (ab) , qui est extérieur. Les droites (ca) et (cb) coupent la conique respectivement en p, q et r, s et les droites (rq) et (ps) se coupent en $m \in (ab)$. On a alors $\sigma_m(a) = b$. En effet, σ_m conserve la droite (ab) et échange p, s et q, r , donc transforme (pq) en (rs) et donc a en b .

3.4.4 Le lemme de Poncelet : cas où la droite (ab) ne coupe pas la conique

Dans cette situation, on peut se ramener au cas du cercle au moyen d'une homographie **réelle**. On considère le plan affine euclidien réel, que l'on plonge dans un plan projectif $\mathbf{P}(E)$, comme complémentaire de la droite D_∞ . On peut ensuite plonger le plan projectif réel dans un plan projectif complexe. Les points "cycliques" $I = (1, i, 0)$ et $J = (1, -i, 0)$ jouent alors un rôle fondamental¹⁰ car ils sont sur tous les cercles (puisque les équations de ceux-ci sont de la forme $x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0$) et qu'ils sont liés à l'orthogonalité par le lemme suivant :

3.4.8 Lemme. *Deux directions $(\alpha, \beta, 0)$ et $(\gamma, \delta, 0)$ sont orthogonales (au sens euclidien) si et seulement si elles sont conjuguées harmoniques par rapport aux points cycliques $I = (1, i, 0)$ et $J = (1, -i, 0)$.*

Démonstration. Nous reverrons ce lemme dans la Partie VI. Pour l'heure, on le vérifie par un calcul sans malice, l'orthogonalité au sens euclidien étant donnée par la nullité du produit scalaire $\alpha\gamma + \beta\delta$.

3.4.9 Remarque. Si on considère le cercle d'équation affine $x^2 + y^2 - 2\alpha x - 2\beta y + \gamma = 0$, il passe par les points cycliques I, J et ses tangentes en ces points sont les droites d'équations $(x - \alpha t) \pm i(y - \beta t) = 0$, c'est-à-dire les droites qui joignent le centre du cercle $o = (\alpha, \beta, 1)$ aux points I et J (ce qu'on appelle les isotropes du point o). En particulier, si l'on a deux cercles concentriques, ils passent par les points cycliques et ont les mêmes tangentes en ces points : ce sont des coniques **bitangentes**, voir 4.2.7.

On a vu ci-dessus qu'il existe une homographie **réelle** $u \in PGL(E)$ telle que $u(\Gamma) = \Gamma'$ soit un cercle et que $u(D) = D' = D_\infty$ (car $D \cap \Gamma = D' \cap \Gamma' = \emptyset$). Les images des points a, b par u sont donc deux directions de droites A, B distinctes. De plus, comme on a supposé a, b non conjugués par rapport à Γ , cela signifie que A, B ne sont pas perpendiculaires en vertu de 2.3.8 et du lemme 3.4.8. Alors, par u , le point p de Γ devient un point p' du cercle Γ' , les points c, d , intersections de Γ avec (pa) et (pb) deviennent $c', d' \in \Gamma'$ et le point m s'envoie sur l'intersection m' des tangentes à Γ' en c', d' . Comme m' décrit un cercle C en vertu de 3.4.3, m décrit la conique $u^{-1}(C)$.

3.4.5 Le lemme de Poncelet : cas général

Dans le cas où la droite $D = (ab)$ coupe la conique Γ en deux points, on ne peut plus envoyer Γ sur un cercle et D sur la droite de l'infini par une homographie réelle (qui, comme toute bijection, conserve le cardinal de l'intersection). On va donc devoir passer par les complexes, mais cela nécessite d'établir un "principe de continuité".

¹⁰Cette situation sera étudiée en détail dans la partie VI.

Le principe de continuité

Voici ce que dit Poncelet à ce sujet :

Quand on se proposera de découvrir quelque propriété générale de position d'une figure, on pourra imaginer que cette figure soit projetée sur un nouveau plan, de telle sorte qu'une ou plusieurs parties de cette figure soient réduites à des circonstances plus simples ; on aura ainsi une nouvelle figure qui pourra remplacer la première, sinon pour toutes les dispositions possibles au moins en général ; on raisonnera sur cette figure comme tenant lieu de la première d'où l'on est parti, et les propriétés, les conséquences générales qu'on en déduira seront également applicables à cette figure, quoiqu'il arrive des cas où la projection soit imaginaire.

Et, un peu plus loin :

Toute propriété de position dont jouit sa projection quand elle est possible, est toujours une propriété de cette figure, même quand la projection est imaginaire.

Une traduction mathématique de ce principe¹¹ nécessite plusieurs préliminaires.

- **Complexification** Chaque espace projectif $\mathbf{P}^n(\mathbf{R})$ se plonge dans son complexifié $\mathbf{P}^n(\mathbf{C})$. Il suffit pour cela de regarder $\mathbf{P}^n(\mathbf{R})$ comme quotient de $\mathbf{R}^{n+1} - \{0\}$ et de plonger \mathbf{R}^{n+1} dans \mathbf{C}^{n+1} .

- **Topologie de Zariski** Cette topologie a été introduite dans la Partie II (voir ??). Elle est définie sur les espaces affines, projectifs, leurs produits et leurs sous-variétés algébriques. Essentiellement, un fermé pour Zariski est une partie définie par des équations polynomiales, une application continue pour Zariski est définie (localement) par des applications polynomiales ou rationnelles.

¹¹Il n'est sans doute pas inutile de rapporter ici les débats suscités par le principe de continuité. Voici qu'en dit Gergonne : *Il faut employer le principe de continuité ... à peu près comme on employait le calcul différentiel lorsqu'on n'en voyait pas bien encore la métaphysique, c'est-à-dire comme instrument de découverte ; mais ce n'en sera pas moins un instrument très précieux, car le plus souvent, en mathématiques, découvrir est tout ; ce ne sont pas d'ordinaire les démonstrations qui embarrassent beaucoup.* Cauchy, dans son rapport à l'Académie de 1820 est plus sévère : *Ce principe n'est, à proprement parler, qu'une forte induction, à l'aide de laquelle on étend des théorèmes établis d'abord à la faveur de certaines restrictions, aux cas où ces mêmes restrictions n'existent plus. ... nous pensons qu'il ne saurait être admis généralement ... En lui accordant trop de confiance, on pourrait tomber quelquefois dans des erreurs manifestes.* Poncelet est ulcéré de ces critiques, qui ne sont sans doute pas exemptes d'arrière-pensées politiques. Voilà ce qu'il en dit, bien plus tard : ... *Monsieur Cauchy, si puissant comme calculateur, si léger et superficiel dans ses jugements ... et, plus loin il se dit : ... profondément humilié et contrarié de tant de retards et de dénis de justice ...*

Avec ces précautions, on peut donner un énoncé :

3.4.10 Proposition. *Soit X une sous-variété algébrique $X \subset \mathbf{P}^{m_1}(\mathbf{C}) \times \cdots \times \mathbf{P}^{m_r}(\mathbf{C})$ et soit F une application définie sur un ouvert de Zariski de X et à valeurs dans un produit $Y = \mathbf{P}^{n_1}(\mathbf{C}) \times \cdots \times \mathbf{P}^{n_s}(\mathbf{C})$. On suppose F continue pour les topologies de Zariski. Soit V une sous-variété algébrique de X , $V_{\mathbf{R}}$ sa partie réelle. On suppose que $V_{\mathbf{R}}$ est dense dans V pour la topologie de Zariski. Alors, si $F(V_{\mathbf{R}})$ est contenu dans une sous-variété algébrique W de Y , il en est de même de $F(V)$.*

Démonstration. C'est la densité : on a $V_{\mathbf{R}} \subset F^{-1}(W)$ donc $V = \overline{V_{\mathbf{R}}} \subset F^{-1}(W)$ car $F^{-1}(W)$ est fermé.

3.4.11 Remarque. La condition de densité est presque toujours satisfaite, sauf dans des cas pathologiques où il y a trop peu de points réels (par exemple le cas d'une conique dégénérée formée de deux droites complexes conjuguées qui n'a qu'un point réel). Voir Partie II, chapitre 7, th. 7.1.2 ou ci-dessous 3.4.16.

Continuité de l'application de Poncelet

Nous allons montrer que la procédure du lemme de Poncelet est continue. On considère une conique Γ et une droite D non tangente à Γ . On associe à un point $p \in \Gamma$ et à deux points distincts $a, b \in D$ le point $m \in \mathbf{P}(E)$ défini selon la procédure de Poncelet : on associe d'abord à (p, a, b) les droites (pa) et (pb) , puis leurs intersections c, d avec Γ , autres que p , puis les tangentes à Γ en c, d et enfin l'intersection m de celles-ci. Si on note $(D \times D)^*$ l'ouvert du produit formé des points (a, b) avec $a \neq b$, notre objectif est donc de prouver :

3.4.12 Proposition. *L'application $F : \Gamma \times (D \times D)^* \rightarrow \mathbf{P}(E)$ qui à (p, a, b) associe m est continue pour les topologies de Zariski.*

Notons déjà que la plupart des opérations géométriques intervenant dans F sont continues pour la topologie de Zariski :

3.4.13 Lemme.

- 1) *L'application d'incidence qui à deux points a, b distincts de $\mathbf{P}(E)$ associe la droite $(ab) \in \mathbf{P}(E^*)$ est continue pour les topologies de Zariski.*
- 2) *L'application d'incidence qui à deux droites A, B distinctes de $\mathbf{P}(E^*)$ associe leur point d'intersection est continue pour les topologies de Zariski.*
- 3) *Soit Γ une conique. L'application qui à un point $a \in \Gamma$ associe la tangente en a , $T_a \in \Gamma^*$ est continue pour les topologies de Zariski.*

Démonstration. 1) On sait que (ab) est définie par la forme linéaire $a \wedge b$ dont les coordonnées sont les 2-mineurs $a_i b_j - a_j b_i$ donc des polynômes en les coordonnées de a, b . Le raisonnement est identique pour les droites A, B .

3) Si l'équation de Γ est $\alpha X^2 + \beta Y^2 + \gamma T^2 + 2\delta YT + 2\epsilon TX + 2\eta XY = 0$, et si on prend $a = (x, y, t)$, l'équation de la tangente est

$$\alpha xX + \beta yY + \gamma tT + \delta(yT + tY) + \epsilon(tX + xT) + \eta(xY + yX) = 0$$

et ses coefficients sont des fonctions polynomiales en x, y, t .

Il ne reste plus, pour achever la preuve de 3.4.12, qu'à examiner les applications du type $(p, a) \mapsto (pa) \mapsto c$, autrement dit l'application qui à un point d'une conique et à une droite passant par ce point associe le deuxième point d'intersection de la droite et de la conique. C'est le lemme calculatoire suivant :

3.4.14 Lemme. *Soit Γ une conique d'équation $\alpha X^2 + \beta Y^2 + \gamma T^2 + 2\delta YT + 2\epsilon TX + 2\eta XY = 0$ et D une droite d'équation $uX + vY + wT = 0$. On suppose que $D \cap \Gamma$ contient $p = (x, y, t)$. Alors, les coordonnées (X, Y, T) du deuxième point d'intersection¹² de D et Γ vérifient les relations suivantes :*

$$\begin{aligned} xX &= \gamma v^2 + \beta w^2 - 2\delta vw, & yY &= \alpha w^2 + \gamma u^2 - 2\epsilon wu, & tT &= \beta u^2 + \alpha v^2 - 2\eta uv, \\ yT + tY &= 2\alpha vw + 2\delta u^2 - 2\epsilon uv - 2\eta wu, & tX + xT &= 2\beta wu + 2\epsilon v^2 - 2\eta vw - 2\delta uv, \\ xY + yX &= 2\gamma uv + 2\eta w^2 - 2\delta wu - 2\epsilon vw. \end{aligned}$$

Pour chaque variable parmi X, Y, T , disons X , les produits $x^2 X, y^2 X, t^2 X$ sont des polynômes homogènes en $\alpha, \beta, \dots, u, v, w$ et x, y, t . L'application qui à $(x, y, t; u, v, w)$ associe (X, Y, T) est continue pour les topologies de Zariski.

Démonstration. Le lecteur est prié de faire lui-même, et sans rechigner, le calcul, facile quoiqu'un peu fastidieux. Une fois en possession des formules ci-dessus, l'assertion sur $x^2 X$, etc. est facile. En effet, la première formule donne $x^2 X$ et pour $y^2 X$ on utilise $y(xY + yX)$ et la formule avec yY . La continuité de l'application est alors immédiate : sur les ouverts du type $D^+(x)$ (l'ouvert de Γ où la coordonnée x est non nulle), elle est bien définie et rationnelle, et ces ouverts recouvrent Γ .

Densité

3.4.15 Remarque. Notons déjà que si une droite ou une conique propre de $\mathbf{P}^2(\mathbf{C})$ a au moins un point à coefficient réels elle en a une infinité. En effet, on peut prendre pour équation $T = 0$ dans le cas de la droite, $Y^2 - XT$ dans le cas de la conique.

¹²Égal à p si D est tangente à Γ en p .

3.4.16 Proposition.

- 1) Si C est une courbe algébrique irréductible complexe (par exemple une droite ou une conique propre), et si A est une partie infinie de C , A est partout dense dans C pour la topologie de Zariski.
- 2) Si X, Y sont des variétés algébriques et si A, B sont Zariski-denses dans X et Y respectivement, $A \times B$ est dense dans $X \times Y$.
- 3) Soient Γ une conique propre et D une droite de $\mathbf{P}^2(\mathbf{C})$. Si Γ et D ont des points réels, l'ensemble des points $(p, a, b) \in \Gamma \times D \times D$ qui sont à coefficients réels et qui vérifient : $a \neq b$, a, b non conjugués par rapport à Γ , (ab) non tangente à Γ , est partout dense dans $\Gamma \times D \times D$.

Démonstration. 1) Cela résulte du fait que les fermés de C pour la topologie de Zariski sont C ou ses parties finies.

2) Quitte à remplacer X, Y par des ouverts denses, on peut supposer que ce sont des variétés affines, plongées respectivement dans k^m et k^n . Les fermés de $X \times Y$ sont alors définis comme ensembles de zéros de fonctions polynomiales $f(x, y)$ avec $x = (x_1, \dots, x_m) \in X$ et $y = (y_1, \dots, y_n) \in Y$. Soit f une telle fonction nulle sur $A \times B$ et fixons $a \in A$. La fonction polynomiale $y \mapsto f(a, y)$ est nulle pour tout $y \in B$ donc, par densité, nulle sur Y . Fixons maintenant $y \in Y$. La fonction $x \mapsto f(x, y)$ est nulle sur A par ce qui précède, donc nulle sur X par densité. On voit que f est nulle sur $X \times Y$ et, comme cela vaut pour toute fonction polynomiale, on a le résultat.

3) Les conditions sur a, b sont des conditions ouvertes pour Zariski, de sorte que l'ensemble des points qui les vérifient est un ouvert dense Ω de $D \times D$. Comme l'ensemble des points réels de $D \times D$ est partout dense dans $D \times D$ en vertu 3.4.15 et de 2), il en est de même des points réels de Ω . On conclut en appliquant 2) avec $X = \Gamma$ et $Y = D \times D$.

Fin de la démonstration

On reprend la situation du lemme de Poncelet. On a donc une conique propre réelle Γ et deux points a, b réels, distincts non situés sur Γ et non conjugués par rapport à Γ . **Comme annoncé, on suppose, de plus, que (ab) n'est pas tangente à Γ .** On considère l'application F décrite ci-dessus et on veut montrer qu'il existe une conique propre réelle C telle que l'image de F soit contenue dans C .

Pour cela, on plonge le plan dans son complexifié. Il existe alors une homographie (complexe) qui envoie Γ sur un cercle Γ' et $D = (ab)$ sur la droite de l'infini D_∞ . On sait que, pour des points réels $p' \in \Gamma'$ et $a', b' \in D_\infty$, le lemme de Poncelet est vrai, c'est-à-dire que $m' = F(p', a', b')$ décrit une conique propre C' (un cercle). Comme les points réels de $\Gamma \times (A \times B)^*$ sont

denses et que F est Zariski-continue, on en déduit que toute l'image de F est contenue dans C' . Par u^{-1} , il en résulte que les points de l'image de F sont dans la conique complexe $C = u^{-1}(C')$. Pour conclure, il faut montrer que l'image est contenue dans une conique réelle. Cela résulte du lemme suivant :

3.4.17 Proposition. *Soit $F(X, Y, T) \in \mathbf{C}[X, Y, T]$ un polynôme homogène de degré d irréductible et non nul. On suppose que l'équation $F = 0$ a une infinité de solutions dans $\mathbf{P}^2(\mathbf{R})$. Alors, il existe $\lambda \in \mathbf{C}$ tel que λF soit à coefficients dans \mathbf{R} .*

Démonstration. On écrit $F = \sum a_{i,j,k} X^i Y^j Z^k$ avec $a_{i,j,k} \in \mathbf{C}$. On note V l'ensemble des $(x, y, t) \in \mathbf{P}^2(\mathbf{R})$ solutions de l'équation $F = 0$. On considère le système d'équations linéaires en les $a_{i,j,k}$ associé aux équations $F(x, y, t) = 0$ pour $(x, y, t) \in V$. Le rang de ce système est indépendant du corps (il est défini par la non nullité de déterminants). Si ce système a une solution $a_{i,j,k}$ non nulle dans \mathbf{C} il en a une aussi dans \mathbf{R} . On a donc un polynôme G à coefficients dans \mathbf{R} homogène de degré d nul sur V . On conclut que $V_{\mathbf{C}}(F) \subset V_{\mathbf{C}}(G)$ par 3.4.16.1, de sorte que G divise F , donc est égal à λF pour une raison de degré.

3.4.18 Remarque. On a vu que les cercles Γ' et C' sont concentriques, donc des coniques bitangentes en les points cycliques. Il en résulte que les coniques Γ et C sont elles aussi bitangentes en les points d'intersection (réels ou non) de la droite (ab) et de Γ .

3.4.19 Commentaire. On voit que la méthode de Poncelet, si elle est très naturelle, nécessite toutefois une mise au point un peu délicate, notamment pour établir rigoureusement le principe de continuité. C'est pourquoi elle a suscité nombre de réactions à l'époque et qu'elle a été discutée, voire décriée.

Une autre méthode, qui a le mérite d'être moins sujette à discussion est donnée ci-dessous.

3.4.6 Une autre preuve du résultat de Poncelet

Le ressort de cette preuve (finalement plutôt plus simple et valable sur tout corps) est la proposition suivante :

3.4.20 Proposition.

1) *Soit Γ une conique propre non vide et soit f une homographie de Γ . Alors, lorsque m varie sur Γ , la droite $(mf(m))$ enveloppe un point ou une conique.*

(Cela signifie que la droite $(mf(m))$ passe par un point fixe ou qu'elle est tangente à une conique fixe Γ' .)

2) Soit Γ^* une conique duale (propre non vide) et soit f une homographie de Γ^* . Alors, lorsque D varie dans Γ^* , le point d'intersection de D et de $f(D)$ décrit une droite ou une conique.

On notera que la deuxième partie de la proposition implique le lemme de Poncelet. En effet, l'application qui à (cm) associe (dm) est une homographie de Γ^* comme composée de l'application tangente-point $(cm) \mapsto c$ (cf. 2.3.5), puis de l'involution de point de Frégier a qui à c associe p , puis de celle de point de Frégier b pour passer à d et enfin de l'application point-tangente $d \mapsto (dm)$.

Démonstration. Par dualité, il suffit de montrer le point 1). On peut supposer que la conique Γ est d'équation $Y^2 - XT = 0$ et on écrit le point m sous la forme $m = (\lambda^2, \lambda\mu, \mu^2)$. Si n est un autre point de Γ on pose $n = (\alpha^2, \alpha\beta, \beta^2)$ et on calcule l'équation $uX + vY + wT = 0$ de la droite (mn) comme $m \wedge n$. En simplifiant¹³ par $\lambda\beta - \mu\alpha$ on trouve $u = \mu\beta$, $v = -(\lambda\beta + \mu\alpha)$ et $w = \lambda\alpha$. Si on a $n = f(m)$ et si l'homographie f , vue comme élément de $PGL(2, k)$, a pour matrice $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, on obtient $u = c\lambda\mu + d\mu^2$, $v = -(c\lambda^2 + (a+d)\lambda\mu + b\mu^2)$ et $w = a\lambda^2 + b\lambda\mu$. On conclut par le lemme suivant :

3.4.21 Lemme. Soient P, Q, R trois polynômes homogènes de degré 2 en λ, μ . Les points de coordonnées homogènes $x = P(\lambda, \mu)$, $y = Q(\lambda, \mu)$, $t = R(\lambda, \mu)$ vérifient une équation $F(x, y, t) = 0$ où F est un polynôme homogène de degré 2.

Démonstration. (du lemme) On cherche F sous la forme $a_1X^2 + a_2Y^2 + a_3T^2 + 2a_4YT + 2a_5TX + 2a_6XY$ avec $a_i \in k$. On écrit que le polynôme $F(P(\lambda, \mu), Q(\lambda, \mu), R(\lambda, \mu))$, homogène de degré 4 en λ, μ , est identiquement nul. Comme il y a cinq monômes $\lambda^4, \lambda^3\mu, \lambda^2\mu^2, \lambda\mu^3$ et μ^4 , on a cinq équations linéaires homogènes en les six inconnues a_i et il y a une solution non nulle.

3.4.22 Remarques. 1) On notera que cette démonstration permet de montrer le lemme de Poncelet y compris dans le cas où la droite (ab) est tangente à la conique, cas que nous avons écarté dans la preuve inspirée de Poncelet.

2) Le calcul précédent montre que (u, v, w) annule un polynôme du second degré donc que la droite $(mf(m))$ enveloppe une conique Γ' , mais cette conique peut être dégénérée. Il y a deux cas *a priori*, celui où Γ' est formé de la

¹³Cette quantité est non nulle si m et n sont distincts et sinon on vérifie que la formule donne bien la tangente en m .

réunion des droites passant par deux points distincts et celui des droites passant par un point compté double. Comme Γ' est l'image de Γ par l'application $m \mapsto (mf(m))$ et que cette application est polynomiale, Γ' est irréductible et le premier cas est impossible.

3) Il reste donc le cas où la droite $(mf(m))$ passe par un point fixe. Cela signifie qu'il existe x, y, t non tous nuls tels que $xP(\lambda, \mu) + yQ(\lambda, \mu) + tR(\lambda, \mu)$ soit identiquement nul. Cette fois on a un système de trois équations à trois inconnues et il faut et il suffit que son déterminant soit nul. Un calcul immédiat montre que ce déterminant est égal à $(ad - bc)(a + d)$. Comme $ad - bc$ est non nul, la condition est donc $a + d = 0$, ce qui signifie que f est une involution (voir Partie I, ??). Bien entendu, le point fixe par lequel passent toutes les droites $(mf(m))$ est alors le point de Frégier de f .

Dans le cas du lemme de Poncelet, l'homographie f est conjuguée du produit des deux involutions de points de Frégier a et b . On sait que c'est une involution si et seulement si les points a, b sont conjugués par rapport à la conique. On retrouve le cas particulier écarté dans 3.4.1.

3.5 Annexe : une généralisation du théorème de Pascal

3.5.1 L'énoncé et ses conséquences

Le but de cette annexe est de prouver une généralisation du théorème de Pascal. Le cadre est l'espace projectif \mathbf{P}_k^2 sur un corps k , avec les coordonnées homogènes x, y, t . On pose $R = k[X, Y, T]$ et on note R_d l'espace vectoriel des polynômes homogènes de degré d . On a $\dim_k R_d = \binom{d+2}{2}$. Rappelons que pour un polynôme homogène $P(X_0, X_1, \dots, X_n)$ on pose :

$$V(P) = \{(x_0, x_1, \dots, x_n) \in \mathbf{P}_k^n \mid P(x_0, x_1, \dots, x_n) = 0\}.$$

Le résultat que nous allons prouver est le suivant :

3.5.1 Théorème. *Soient $A, B, F, G \in R$ des polynômes homogènes de degrés respectifs a, b, s, t positifs. On suppose que A et B sont premiers entre eux, que $S = V(A) \cap V(B)$ est fini de cardinal ab , que F et G sont premiers entre eux, que $Z = V(F) \cap V(G)$ est fini de cardinal st et que S est inclus dans Z . Alors il existe $H \in R$, homogène de degré $s + t - a - b$ (et donc non nul) tel que $Z - S \subset V(H)$.*

Ce théorème implique le théorème de Pascal (et celui de Pappus) :

3.5.2 Corollaire. Soit Γ une conique propre de \mathbf{P}_k^2 (resp. la réunion de deux droites D et D' sécantes en o) et soient p, q, r, p', q', r' des points distincts de Γ (resp. $p, q, r \in D, p', q', r' \in D'$ des points distincts de o). Les droites (qr') et $(q'r)$ (resp. (rp') et $(r'p)$, resp. (pq') et $(p'q)$) se coupent en u (resp. v , resp. w). Alors, u, v, w sont alignés.

Démonstration. (du corollaire) Dans ce qui suit on identifie une courbe et son équation. On applique 3.5.1 avec $A = \Gamma$ (resp. $A = DD'$), $B = (qr')(rp')(pq')$ (c'est l'équation de degré 3 qui définit la réunion des trois droites), $F = B$ et $G = (q'r)(r'p)(p'q)$. L'ensemble S est formé des 6 points p, q, r, p', q', r' , l'ensemble Z contient en plus u, v, w . Il est clair que A et B (resp. F et G) sont premiers entre eux. Comme on a $a = 2, b = s = t = 3$, donc $s + t - a - b = 1$, les points u, v, w sont alignés.

3.5.3 Remarques.

- 1) Les hypothèses A et B (resp. F et G) premiers entre eux seront discutées plus loin. Elles sont souvent inutiles (par exemple si k est un corps algébriquement clos, ou le corps des réels), mais elles peuvent être en défaut sur un corps fini, cf. 3.5.20, 3.5.24. Dans le cas d'un corps infini quelconque, j'ignore si elles sont nécessaires.
- 2) On voit que le théorème 3.5.1 est beaucoup plus général que le théorème de Pascal. Il a pour conséquence de nombreux autres résultats. Nous verrons notamment ci-dessous une application aux cubiques, voir 3.5.25. On en trouvera d'autres dans [Ful69] Ch. 5, §6.
- 3) On notera que la géométrie impose des contraintes sur les nombres a, b, s, t . En effet, dans la configuration précédente, on a non seulement $ab < st$, mais aussi $a + b < s + t$, ce qui n'est automatique *a priori*. Cela montre, par exemple, que l'intersection d'une conique et d'une courbe de degré 4, bien que formée de 8 points, ne peut être contenue dans l'intersection de deux cubiques qui contient pourtant 9 points.
- 4) Si l'on fait vraiment de la géométrie algébrique, i.e. si utilise le langage des schémas, on n'est pas obligé de supposer les points de S et Z distincts, il peut y avoir des multiplicités.
- 5) En fait, ce théorème est un résultat de liaison : S et $Z - S$ sont des groupes de points "liés" par l'intersection complète $Z = V(F) \cap V(G)$ (cela signifie que leur réunion est Z), cf. [Per95], [CP74], [DP90], etc.

3.5.2 La démonstration du théorème de Pascal généralisé

Le théorème de Noether

La preuve de 3.5.1 repose essentiellement sur le résultat suivant, qui calcule les équations d’une “intersection complète”. Il s’agit de la forme faible du théorème dit $AU + BV$ de Max Noether, cf. [Ful69] Ch. 5, §5.

3.5.4 Théorème. *Soient $A, B \in R$ des polynômes homogènes de degrés respectifs a, b . On suppose que $S = V(A) \cap V(B)$ est fini de cardinal ab et que A et B sont premiers entre eux. Alors les polynômes homogènes de degré d nuls sur S sont les polynômes de la forme $AU + BV$ avec U, V homogènes de degrés respectifs $d - a$ et $d - b$. (Autrement dit, l’idéal $I = I(S)$ des polynômes nuls sur S est égal à l’idéal J engendré par A et B .)*

Fin de la démonstration de 3.5.1

Admettons un instant le théorème de Noether et finissons de prouver 3.5.1.

Comme F et G sont nuls sur S ils s’écrivent, en vertu du théorème de Noether, $F = AU + BV$, $G = AU' + BV'$ avec U, V, U', V' respectivement homogènes de degrés $s - a, s - b, t - a, t - b$. On considère alors le polynôme $H = UV' - VU'$. On a $AH = V'(AU + BV) - V(AU' + BV') = V'F - VG$ et, de même, $BH = UG - U'F$.

Montrons d’abord que H n’est pas le polynôme nul. Les polynômes U, V, U', V' ne sont pas tous nuls, supposons par exemple $V \neq 0$. Si H était nul on aurait $AH = 0$, donc $VG = V'F$, mais comme F et G sont premiers entre eux, le théorème de Gauss montre que F diviserait V ce qui est absurde car on a $\deg V < \deg F$ et $V \neq 0$.

Le polynôme H est donc homogène de degré $s + t - a - b$. Il reste à voir qu’il est nul sur $Z - S$. Il est clair que AH et BH sont nuls sur Z . Si le point p est dans $Z - S$ il annule AH et BH , mais, comme il n’annule pas à la fois A et B (puisqu’il n’est pas dans S), il annule H .

3.5.5 Remarque. La démonstration ci-dessus n’est autre que le calcul de la résolution d’un “lié”, cf. [Per95] Ch. X, th. 3.8, [CP74], etc.

3.5.3 La démonstration du théorème de Noether

Cette démonstration nécessite quelques étapes et elle comporte quelques pièges dans le cas d’un corps quelconque, ce qui nous a conduit à préférer une preuve par réduction au cas algébriquement clos.

Le cas k algébriquement clos : préliminaires

Les quelques lemmes suivants expliquent l'intérêt de travailler sur un corps algébriquement clos :

3.5.6 Lemme. *On suppose k infini (par exemple algébriquement clos). Soit $P \in k[X, Y, T]$ un polynôme homogène. Si $V(P)$ est égal à \mathbf{P}_k^2 , P est le polynôme nul.*

Démonstration. Il s'agit de montrer que si P est non nul il ne s'annule pas sur \mathbf{P}^2 tout entier. Le cas où P est constant étant trivial on peut supposer que P est de degré > 0 et, par exemple, que la variable T apparaît avec un degré $r > 0$. On écrit alors $P(X, Y, T) = a_r(X, Y)T^r + \dots + a_0(X, Y)$ avec $a_r(X, Y)$ homogène de degré $d \geq 0$ et non nul. Le polynôme a_r s'écrit à son tour $a_r(X, Y) = \sum_{i=0}^d \alpha_i X^i Y^{d-i}$ où les α_i ne sont pas tous nuls. Le polynôme $a_r(X, 1)$ est un polynôme en une variable, non nul, donc il a un nombre fini de racines. Soit $x \in k$ un nombre qui n'annule pas $a_r(X, 1)$ (il en existe car k est infini). Le polynôme $P(x, 1, T)$ est alors un polynôme de degré r en T . Il a au plus r racines et il existe donc t tel que $P(x, 1, t)$ soit non nul.

3.5.7 Remarque. Bien entendu ce résultat est faux sur un corps fini. Par exemple le polynôme $TX^p - XT^p$ est nul sur \mathbf{P}^2 dans le cas $k = \mathbf{F}_p$ en vertu du petit théorème de Fermat. Voir aussi Partie II ??.

3.5.8 Lemme. *On suppose k algébriquement clos. Soit $P(X, Y, T)$ un polynôme homogène de degré > 0 . Alors, $V(P)$ est infini.*

Démonstration. Il suffit de reprendre la preuve de 3.5.6 en notant qu'il y a une infinité de x tels que $a_r(x, 1)$ soit non nul. Pour chacun de ces x , le polynôme $P(x, 1, T)$ est de degré $r > 0$ en T , donc il admet au moins une racine (car k est algébriquement clos). On obtient ainsi une infinité de points de $V(P)$.

3.5.9 Remarques.

- 1) Ce résultat n'est pas vrai en général sur un corps infini comme on le voit en considérant par exemple les polynômes $X^2 + Y^2 + T^2$ ou $X^2 + Y^2$ sur \mathbf{R} .
- 2) Ce résultat montre que, sur un corps algébriquement clos, les hypothèses faites dans 3.5.1 ou 3.5.4 : " A et B (resp. F et G) premiers entre eux" sont superflues. En effet, si C est un diviseur de degré > 0 de A et B , $V(C)$ est infini et est contenu dans $V(A) \cap V(B)$ ce qui est absurde.

Le cas algébriquement clos avec $d \geq ab - 1$

On commence par montrer 3.5.4 dans le cas $d \geq ab - 1$. On a encore besoin de deux lemmes :

3.5.10 Lemme. Soit r un entier ≥ 1 et $S = \{s_1, \dots, s_r\}$ un ensemble fini de cardinal r de k^3 , avec $s_i = (x_i, y_i, t_i)$ et soit d un entier avec $d \geq r - 1$.

1) Pour tout $i = 1, 2, \dots, r$, il existe un polynôme $F_i(X, Y, T)$, homogène de degré d , tel que $F_i(s_i) \neq 0$ et $F_i(s_j) = 0$ pour tout $j \neq i$.

2) Soit $\varphi : R_d \rightarrow k^r$ l'application linéaire qui à F associe le r -uplet des $F(x_i, y_i, t_i)$. Alors, φ est surjective.

Démonstration. 1) Quitte à effectuer une homographie, on peut supposer $s_i = (0, 0, 1)$. Si on pose $s_j = (x_j, y_j, t_j)$ l'un des nombres x_j ou y_j est non nul. On considère alors le polynôme P_j égal à $T - \frac{t_j}{x_j}X$ (resp. $T - \frac{t_j}{y_j}Y$) si $x_j \neq 0$ (resp. si $y_j \neq 0$). Il est clair que $F_i = T^{d-r+1} \prod_{j \neq i} P_j$ convient.

2) Quitte à multiplier par un scalaire, le polynôme F_i s'envoie par φ sur le i -ème vecteur de la base canonique de k^r .

3.5.11 Lemme. Soit J l'idéal de R engendré par A et B . On a "une résolution" de J , c'est-à-dire une suite exacte :

$$0 \rightarrow R \xrightarrow{\beta} R \times R \xrightarrow{\alpha} J \rightarrow 0$$

avec $\alpha(U, V) = AU + BV$ et $\beta(W) = (BW, -AW)$. Précisément, pour $d \geq 0$, on a la suite exacte :

$$0 \rightarrow R_{d-a-b} \xrightarrow{\beta} R_{d-a} \times R_{d-b} \xrightarrow{\alpha} J_d \rightarrow 0$$

où J_d est l'espace vectoriel des polynômes homogènes de degré d de J .

Démonstration. Il s'agit de montrer que si l'on a $AU + BV = 0$, alors on a $(U, V) = (BW, -AW)$. Cela résulte du fait que A et B sont premiers entre eux et du théorème de Gauss. Le complément est la traduction du résultat sur les polynômes homogènes.

3.5.12 Corollaire. On suppose¹⁴ $d \geq a + b$. On a

$$\dim J_d = \binom{d-a+2}{2} + \binom{d-b+2}{2} - \binom{d-a-b+2}{2} = \binom{d+2}{2} - ab.$$

¹⁴Le lecteur vérifiera qu'il suffit de supposer $d \geq a + b - 2$.

Démonstration. La première égalité résulte du lemme précédent par application de la formule $\dim_k R_n = \binom{n+2}{2}$. La seconde se montre par un calcul sans difficulté.

On peut alors prouver 3.5.4 dans le cas $d \geq ab - 1$. Il est clair que l'espace vectoriel J_d des polynômes de degré d de la forme $UA + VB$ est inclus dans I_d . En vertu de¹⁵ 3.5.12 on a $\dim J_d = \binom{d+2}{2} - ab$. Par ailleurs, avec les notations de 3.5.10, I_d est le noyau du morphisme φ de R_d dans k^{ab} associé à $S = V(A) \cap V(B)$ et, comme ce morphisme est surjectif en vertu de 3.5.10, le noyau a même dimension que J_d , d'où le résultat.

Le cas algébriquement clos avec $d < ab - 1$

Il reste à prouver le théorème 3.5.4 dans le cas $d < ab - 1$. Soit F un polynôme homogène de degré d nul sur S . Soit m un point n'appartenant pas à S . Il existe une droite D passant par m qui ne passe par aucun point de S (comme k est infini, il y a une infinité de droites passant par m et seulement un nombre fini d'entre elles contiennent des points de S). L'équation de D est une forme linéaire L qui ne s'annule en aucun point de S . Alors, pour n assez grand, $L^n F$, qui s'annule sur S , est dans J en vertu du premier cas. Il ne reste plus qu'à montrer le lemme suivant :

3.5.13 Lemme. *Avec les notations de 3.5.4, soit L une forme linéaire qui ne s'annule pas sur S . Alors la multiplication par L :*

$$\mu_L : R/(A, B) \rightarrow R/(A, B)$$

est injective.

Démonstration. Soit F tel que $LF = AU + BV$. Il s'agit de voir que F est encore de cette forme. Quitte à faire une homographie on peut supposer $L = T$. On réduit alors modulo T et on a $\overline{AU} = -\overline{BV}$. Mais les polynômes $\overline{A}, \overline{B} \in k[X, Y]$, sont premiers entre eux. En effet¹⁶, sinon, cf. 3.5.9.2, A et B auraient un zéro commun sur la droite $T = 0$. On en déduit, par Gauss, que \overline{A} divise \overline{V} : $\overline{V} = \overline{AC}$ et il s'ensuit $\overline{U} = -\overline{BC}$. Revenant dans R , cela donne $V = AC + TV'$ et $U = -BC + TU'$, d'où $TF = T(AU' + BV')$ et la conclusion.

¹⁵On vérifie que $d \geq ab - 1$ implique $d \geq a + b - 2$.

¹⁶C'est ici, et seulement ici, qu'on utilise le fait que k est algébriquement clos. Le lemme utilisé est le suivant. Soient A, B deux polynômes homogènes de degrés a, b de $k[X, Y, T]$, premiers entre eux. Il existe une forme linéaire L telle que les polynômes \overline{A} et \overline{B} réduits modulo L soient encore premiers entre eux. Il est encore vrai sur un corps infini, mais le plus simple pour le prouver est de se ramener au cas algébriquement clos. Sur un corps fini il peut être faux, exemple, $k = \mathbf{F}_3$, $A = XT(X + T)(X - T)$ et $B = Y$.

Réduction au cas où k est algébriquement clos

Montrons maintenant 3.5.4 dans le cas général. La réduction utilise des techniques déjà rencontrées Partie II dans la preuve de ???. On plonge k dans un corps algébriquement clos \bar{k} (c'est le théorème de Steinitz, cf. par exemple [Lan69] Ch V, Th. 2.5). On choisit une base $(e_i)_{i \in I}$ du k -espace vectoriel \bar{k} (cf. [Lan69] Ch. III, Th. 5.1), avec $e_0 = 1$. En écrivant les polynômes comme combinaison linéaires de monômes, on en déduit que $\bar{k}[X, Y, T]$ est un $k[X, Y, T]$ -module libre de base $(e_i)_{i \in I}$.

On a besoin de deux résultats auxiliaires :

3.5.14 Lemme. Bézout, forme faible Soient $A, B \in k[X, Y, T]$ deux polynômes homogènes de degrés a, b , premiers entre eux. On a $|V(A) \cap V(B)| \leq ab$.

Démonstration. Voir [Ful69] ou exercice 4.6.6 ci-dessous.

3.5.15 Lemme. Avec les notations de 3.5.4, si A et B sont premiers entre eux dans $k[X, Y, T]$ ils le sont encore dans $k(X, Y)[T]$ et dans $\bar{k}[X, Y, T]$.

Démonstration. Montrons d'abord que les polynômes A, B sont encore premiers entre eux dans $k(X, Y)[T]$. Sinon on a un diviseur commun $C : A = CA', B = CB'$ avec $C, A', B' \in k(X, Y)[T]$. On peut écrire $C = \frac{c}{d}C_0$ avec $c, d \in k[X, Y]$ premiers entre eux et $C_0 \in k[X, Y, T]$, polynôme en T dont les coefficients sont des polynômes en X, Y premiers entre eux (voir par exemple [Per96] Ch. II, Prop. 4.4). Il s'agit de voir que C est de degré 0 en T . Sinon, on écrit, de même, $A' = \frac{a'}{d}A'_0$ et $B' = \frac{b'}{d}B'_0$. Comme C_0 est premier avec d (sinon, ses coefficients auraient un facteur commun non trivial), le théorème de Gauss montre que C_0 divise A et B donc est une constante, de sorte que C est bien dans $k(X, Y)$.

On écrit alors la relation de Bézout dans l'anneau principal $k(X, Y)[T] : UA + VB = 1$ et, en chassant les dénominateurs, on obtient $U'A + V'B = C(X, Y)$. On a évidemment des relations analogues en T, X et Y, T . Supposons maintenant que $D(X, Y, T)$ divise A et B dans $\bar{k}[X, Y, T]$. On voit que D divise le polynôme $C(X, Y)$ donc est de degré nul en T . Mais, le même raisonnement montre qu'il est de degré nul en X et Y , donc une constante.

Reprenons alors la preuve de Noether. Sur \bar{k} , A et B sont encore premiers entre eux en vertu de 3.5.15, donc ils ont au plus ab zéros communs dans \mathbf{P}^2 par 3.5.14, donc exactement ab (puisque ces zéros sont déjà dans k). On peut donc appliquer Noether à A, B, F sur \bar{k} . Il existe $U, V \in \bar{k}[X, Y, T]$ avec $F = AU + BV$. Mais, si on écrit $U = \sum_{i \in I} U_i e_i$, $V = \sum_{i \in I} V_i e_i$, avec $U_i, V_i \in k[X, Y, T]$, l'identification des coefficients donne $F = U_0 A + V_0 B$.

Une preuve élémentaire de Noether dans le cas de Pascal

Dans ce paragraphe nous donnons une preuve directe de Noether dans le cas qui nous intéresse, celui de Pascal¹⁷, par des moyens élémentaires, sur un corps quelconque de cardinal > 5 et sans utiliser d'hypothèse de primalité relative de A et B .

On commence par un résultat presque évident :

3.5.16 Lemme. *Soit $H(u, v)$ un polynôme homogène de degré d (non nul). Alors $V(H)$ est de cardinal $\leq d$. En particulier, si H est nul sur \mathbf{P}_k^1 et si on a $|k| \geq d$, le polynôme H est le polynôme nul.*

Démonstration. On écrit $H(u, v) = \sum_{i=0}^d a_i u^i v^{d-i}$. Les points de $V(H)$ sont le point $(1, 0)$ (si $a_d = 0$) et les points $(x, 1)$ avec $x \in k$ racine de $a_d x^d + \dots + a_1 x + a_0 = 0$. Il y a bien, en tout, d points au plus.

On enchaîne par une forme faible du Nullstellensatz :

3.5.17 Lemme. *Soit A un polynôme homogène de degré 2. On suppose que la conique associée $V(A)$ est propre et non vide. Soit G un polynôme homogène de degré d nul sur $V(A)$. On suppose $|k| \geq 2d$. Alors, G est multiple de A .*

Démonstration. Quitte à faire une homographie on peut supposer $A = Y^2 - XT$. On effectue la division euclidienne de G par le polynôme A considéré comme polynôme unitaire en Y à coefficients dans $k[X, T]$. On a donc :

$$G(X, Y, T) = A(X, Y, T)Q(X, Y, T) + a(X, T)Y + b(X, T)$$

où a et b sont homogènes de degrés $d - 1$ et d . La paramétrisation de $V(A)$ fournit la bijection $\pi : \mathbf{P}_k^1 \rightarrow V(A)$, donnée par $\pi(u, v) = (u^2, uv, v^2)$ et, comme G est nul sur $V(A)$, on a $a(u^2, v^2)uv + b(u^2, v^2) = 0$ pour tous $(u, v) \in \mathbf{P}_k^1$. Le polynôme $a(u^2, v^2)uv + b(u^2, v^2)$, qui est de degré $2d$, est donc le polynôme nul en vertu de 3.5.16. L'identification des termes de degré impair (resp. pair) en u montre alors que a et b sont nuls. On a bien $G = AQ$ comme annoncé.

On montre ensuite une variante de Bézout :

3.5.18 Théorème. *On suppose $|k| > 5$. Soient A, G des polynômes homogènes de degrés respectifs 2 et 3. On suppose A irréductible (“une conique propre”) et G non multiple de A . Alors on a $|V(A) \cap V(G)| \leq 6$.*

Démonstration. Le résultat est évident si la conique $V(A)$ est vide. Sinon, par changement de repère on peut supposer $A = Y^2 - XT$, on a comme ci-dessus

¹⁷Le lecteur montrera, par la même méthode, un résultat analogue pour le cas de Pappus.

la bijection $\pi : \mathbf{P}_k^1 \rightarrow V(A)$, donnée par $\pi(u, v) = (u^2, uv, v^2)$ et $\pi(u, v)$ est dans $V(A) \cap V(G)$ si et seulement si on a $\overline{G}(u, v) := G(u^2, uv, v^2) = 0$. Le polynôme \overline{G} est homogène de degré 6 en u, v et il a donc au plus 6 zéros dans \mathbf{P}^2 sauf s'il est nul (cf. 3.5.16). Mais, si \overline{G} est nul, cela signifie que $V(A)$ est inclus dans $V(G)$ ce qui impose que A divise G en vertu de 3.5.17.

On en déduit Noether (le lecteur notera qu'on ne fait pas l'hypothèse que A et B sont premiers entre eux) :

3.5.19 Théorème. *On suppose $|k| > 5$. Soient A, B homogènes de degrés 2 et 3. On suppose que $V(A)$ est une conique propre (i.e. que A est irréductible) et que $S = V(A) \cap V(B)$ est de cardinal 6. Soit F homogène de degré 3 nul sur S . Alors F est de la forme $AU + vB$, avec U de degré 1 et v constant.*

Démonstration. Soit p un point de $V(A)$ non dans S (il en existe car $V(A)$ est de cardinal $|k| + 1 > 6$). On a donc $B(p) \neq 0$, de sorte qu'il existe $v \in k$ tel que $F(p) - vB(p) = 0$. Posons $G = F - vB$. Alors $V(A) \cap V(G)$ contient 7 points (ceux de S , plus p). Il résulte alors de 3.5.18 que G est multiple de A , $G = UA$, cqfd.

3.5.20 Remarque. Les résultats précédents peuvent être en défaut pour des corps de cardinal ≤ 5 . Par exemple, sur \mathbf{F}_5 , si on prend $A = Y^2 - XT$, $V(A)$ est de cardinal 6 = 5 + 1 (c'est une conique propre) et formé des points $(0, 0, 1)$, $(1, 0, 0)$, $(1, 1, 1)$, $(1, -1, 1)$, $(-1, -2, 1)$ et $(-1, 2, 1)$. Le polynôme $F = Y(X - T)(X + T)$ est nul sur cet ensemble, mais n'est pas multiple de A , ce qui met en défaut 3.5.17. De plus, si on prend $B = X(Y^2 - XT)$, on a $V(A) \cap V(B) = V(A)$, mais F , qui est nul sur cet ensemble, n'est pas dans l'idéal $(A, B) = (A)$, ce qui contredit Noether.

Discussion sur les hypothèses de 3.5.1

Nous avons vu plus haut que, sur un corps algébriquement clos, la condition $V(A) \cap V(B)$ fini implique que A et B sont premiers entre eux, de sorte que cette hypothèse est superflue dans 3.5.1. Sur corps des réels c'est encore le cas, précisément on a le résultat suivant :

3.5.21 Proposition. *On suppose $k = \mathbf{R}$. Soient A, B des polynômes homogènes de degré a et b tels que $|V(A) \cap V(B)| = ab$. Alors A et B sont premiers entre eux.*

Démonstration. On utilise le lemme suivant, voir l'article *Real Zeros of Positive Semidefinite forms* de Choi-Lam-Reznick dans Math. Zeitschrift 171 (1980) :

3.5.22 Lemme. Soit $F \in \mathbf{R}[X, Y, T]$ un polynôme homogène de degré d . Si $V(F)$ est fini on a $|V(F)| \leq \frac{d^2}{2}$.

Revenons à la proposition. Si A et B ont un facteur commun C on a $A = CA'$, $B = CB'$ avec A', B' premiers entre eux. Posons $c = \deg C$, $a' = \deg A'$, $b' = \deg B'$ et supposons $c > 0$. On a $V(A) \cap V(B) = V(C) \cup (V(A') \cap V(B'))$. Le lemme précédent, associé à Bézout, donne $|V(A) \cap V(B)| \leq \frac{c^2}{2} + a'b' < ab = c^2 + a'b' + c(a' + b')$ et c'est absurde.

3.5.23 Remarque. On a vu ci dessus (cf. 3.5.20) que Noether peut être faux sur un corps fini de cardinal trop petit par rapport aux degrés des polynômes sans l'hypothèse “ A et B premiers entre eux”. Dans le cas d'un corps infini j'ignore si Noether est toujours vrai sans cette hypothèse et si l'on a encore un analogue du lemme 3.5.22. On arrive là aux confins de Mordell-Weil, Faltings et autres, alors ...

3.5.24 Remarque. Même si Noether est vrai, la généralisation du théorème de Pascal peut être fausse si l'hypothèse F, G premiers entre eux n'est pas réalisée. Voici un contre-exemple. On prend $k = \mathbf{F}_7$ et pour A une conique propre non vide. On a donc $|V(A)| = 8$. On choisit 6 points x_1, \dots, x_6 de cette conique et on prend pour B la réunion des droites (x_1x_2) , (x_3x_4) et (x_5x_6) . On a donc $V(A) \cap V(B) = \{x_1, \dots, x_6\}$ et cet ensemble est de cardinal 6. Soient a, b les deux derniers points de $V(A)$ et soit c un point qui n'est situé ni sur $V(A)$, ni sur (ab) (un calcul de cardinal montre qu'il y a 43 points c possibles). On considère deux droites d'équations X, Y passant par c et on pose $F = XA$, $G = YA$. On a alors $Z = V(F) \cap V(G) = V(A) \cup \{c\}$, cet ensemble est de cardinal 9, il contient $S = V(A) \cap V(B)$, mais les points qui ne sont pas dans S sont a, b, c qui ne sont pas alignés.

3.5.4 Une application : loi de groupe sur une cubique plane

Ce paragraphe sera utile pour démontrer le grand théorème de Poncelet au chapitre suivant. On travaille sur un corps k infini. et on utilise quelques notions sur les courbes algébriques pour lesquelles le lecteur est renvoyé à [Per95], [Ful69], [Har77], etc.

Rappelons qu'un point $p = (x, y, t)$ d'une courbe algébrique d'équation homogène $F(X, Y, T) = 0$ est dit **singulier** s'il annule aussi les dérivées partielles $\partial F / \partial X$, $\partial F / \partial Y$ et $\partial F / \partial T$. Si F est de degré 3 et si p est le point $(0, 0, 1)$ cela signifie que les termes en T^3 et T^2 de F sont nuls. Une courbe sans point singulier est dite **non singulière**.

Qui passe par huit passe par neuf

3.5.25 Proposition. Soient $A, B \in R = k[X, Y, T]$ des polynômes homogènes de degré 3. On suppose le polynôme A irréductible, la courbe $V(A)$ non singulière et A et B non proportionnels¹⁸. On suppose que $S = V(A) \cap V(B)$ est de cardinal 9. Soit F un polynôme de degré 3 tel que $V(F)$ contient 8 points de S . Alors $V(F)$ contient S tout entier.

Démonstration. Posons $S = \{a_1, \dots, a_9\}$ et supposons que $V(F)$ contient a_1, \dots, a_8 . On a le lemme suivant :

3.5.26 Lemme. Il existe un polynôme L , homogène de degré 1 tel que, dans une extension k' de k , $V(A) \cap V(L)$ contient trois points distincts a_9, b, c , avec $b, c \notin V(B)$.

Démonstration. Quitte à changer de repère, on peut supposer $a_9 = (0, 0, 1)$. Le polynôme A s'écrit sous la forme $P(X, Y) + Q(X, Y)T + R(X, Y)T^2$ avec P, Q, R homogènes de degrés respectifs 3, 2, 1. Comme A est irréductible, P est non nul, comme $V(A)$ est non singulière, R est non nul. De plus, le discriminant $\Delta(X, Y) = Q^2 - 4PR$ est non nul lui aussi (sinon on a $4RA = (2TR + Q)^2$ et cela contredit l'irréductibilité de A).

On cherche L sous la forme $Y - \lambda X$ avec $\lambda \in k$. Il n'y a qu'un nombre fini de λ tels que L passe par un des points a_1, \dots, a_8 . Comme k est infini, on peut écarter ces valeurs. Les points d'intersection de $V(A)$ et $V(L)$ autres que a_9 sont donnés par l'équation : $X^2P(1, \lambda) + XTQ(1, \lambda) + T^2R(1, \lambda) = 0$. On élimine les λ qui annulent $P(1, \lambda)$ ou $Q(1, \lambda)$ ou $\Delta(1, \lambda)$ et qui sont en nombre fini. Il reste une infinité de λ pour lesquels on a une équation de degré 2, qui admet 2 racines distinctes dans une extension quadratique de k et ces racines donnent deux points b, c distincts des a_i . Il en résulte que b, c ne sont pas dans $V(B)$. Sinon, $V(A) \cap V(B)$ aurait plus de 9 points. En vertu de 3.5.14, cela implique que A, B ont un facteur commun, et, comme A est irréductible, qu'ils sont proportionnels, ce qui a été écarté.

Revenons à la proposition. On choisit un polynôme L comme ci-dessus et on considère le polynôme LF . Il est nul en tous les a_i . En vertu de 3.5.4, il s'écrit $LF = AU + BV$ avec U, V de degré 1. Comme b, c annulent L et A et pas B , ils annulent V . Comme b, c sont distincts, les droites d'équations L et V sont égales. Il s'ensuit que L divise AU . Comme il ne divise pas A (qui

¹⁸Cette hypothèse n'est utile que dans le cas où A et B sont proportionnelles et où le cardinal de $V(A)$ est égal à 9. Pour voir qu'il existe effectivement des courbes elliptiques sur \mathbf{Q} de cardinal 9, voir par exemple *Daniel S. Kubert, Universal bounds on the torsion of elliptic curves, Proc. London Math. Soc. (3) 33 (1976), 193-237*. Cela étant, il est possible que, même dans ce cas, l'hypothèse ne soit pas indispensable ...

est irréductible), il divise U . Mais alors, F est combinaison linéaire de A et B donc nul en a_9 .

La loi de groupe sur une cubique plane

Rappelons que si Γ est une cubique plane non singulière et D une droite, l'intersection $D \cap \Gamma$ contient au plus trois points (éventuellement confondus), que si elle en contient deux elle en contient trois et que, si elle est tangente à Γ en P , elle recoupe Γ en Q , distinct de P , sauf si P est un point d'inflexion de Γ .

On considère une cubique plane Γ , non singulière, d'équation F (c'est ce qu'on appelle une **courbe elliptique**¹⁹). On choisit un point $O \in \Gamma$. On définit une loi de composition sur Γ , notée \oplus , de la manière suivante. Soient P, Q deux points de Γ . On considère la droite²⁰ (PQ) . Elle recoupe Γ en un point noté $P \vee Q$. On considère la droite joignant O et $P \vee Q$. Elle recoupe Γ en R et on pose $R = P \oplus Q$.

3.5.27 Théorème. *L'ensemble Γ , muni de la loi \oplus , est un groupe abélien d'élément neutre O .*

Démonstration. La commutativité est claire, ainsi que le fait que O est élément neutre. Pour trouver l'opposé de P , on considère la tangente à Γ en O . Elle recoupe Γ en Q . Le point $-P$ est le point où (PQ) recoupe Γ .

3.5.28 Remarques.

- 1) On prend souvent comme origine un point d'inflexion de Γ . L'opposé de P est alors le point où (OP) recoupe Γ .
- 2) On montre (voir par exemple [Hus87] ou [Sil86] ...) qu'une cubique plane non singulière peut s'écrire, dans un repère convenable, sous la forme $Y^2T = P(X, T)$ où le polynôme $P(x, 1)$, de degré 3, a trois racines distinctes dans une extension de k . Dans ce cas, on prend souvent comme origine le point à l'infini $(0, 1, 0)$ qui est un point d'inflexion. L'opposé de $P = (x, y, t)$ est alors $(x, -y, t)$.

Il reste à montrer l'associativité, qui est moins évidente. Soient P, Q, R trois points de Γ . On pose, voir figure ci-dessous, $S = P \vee Q$, $T = P \oplus Q = S \vee O$, $U = T \vee R$, $V = Q \vee R$, $W = Q \oplus R = V \vee O$, $X = P \vee W$. On a $(P \oplus Q) \oplus R = U \vee O$ et $P \oplus (Q \oplus R) = X \vee O$. Pour montrer l'associativité, il suffit donc de montrer l'égalité $U = X$.

¹⁹La théorie des courbes elliptiques est l'un des paradis des mathématiciens et la littérature autour de ce thème est très abondante.

²⁰Dans tout ce qui suit, lorsque les points P, Q coïncident, on convient que la droite (PQ) est la tangente à Γ en P .

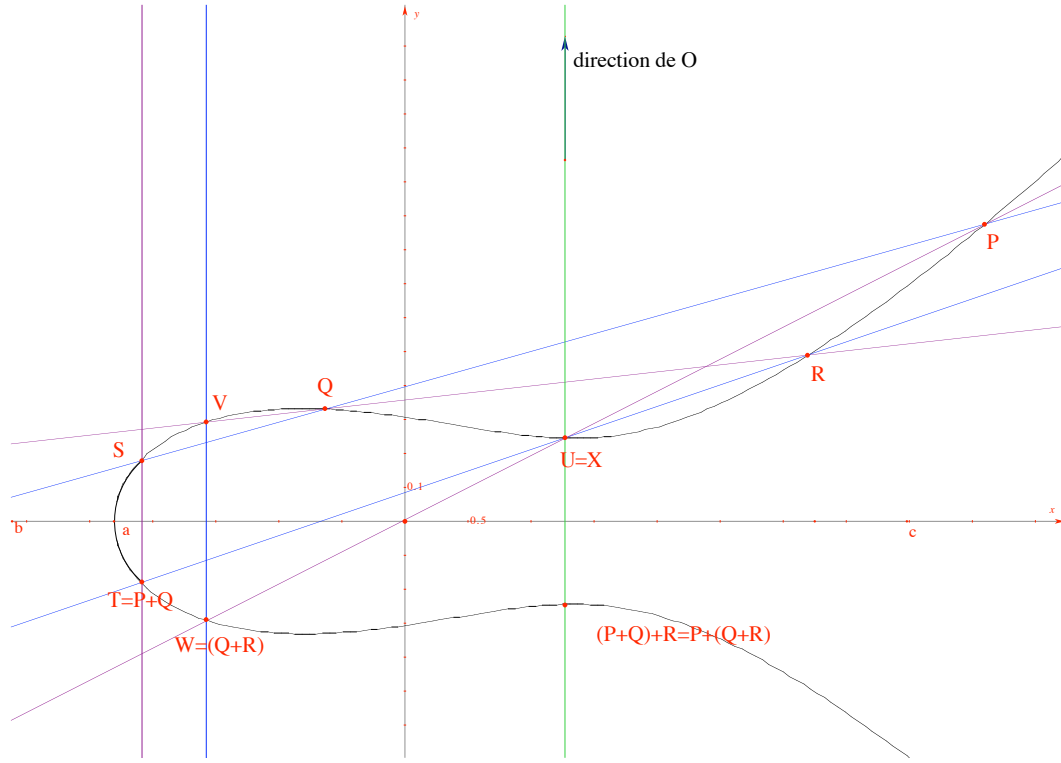


Figure 3.12: L'associativité de la loi de groupe.

Supposons d'abord que tous les points cités ci-dessus sont distincts. On considère les droites $L = (PQS)$, $L' = (OST)$, $M = (TUR)$, $M' = (QRV)$, $N = (OVW)$, $N' = (PWX)$ et les cubiques $C = LMN$ et $C' = L'M'N'$. L'intersection de Γ et C est formée des neuf points $P, Q, S, T, U, R, O, V, W$, tandis que celle de Γ et C' est formée des mêmes points sauf U qui est remplacé par X . En vertu de 3.5.25, $C' \cap \Gamma$ contient aussi U qui est donc bien égal à X .

Pour le cas général, on écrit la cubique sous la forme $Y^2T = P(X, T)$ évoquée ci-dessus et on utilise le principe de prolongement des identités algébriques, ou encore l'irréductibilité de Γ . On pose $P = (x_1, y_1, t_1)$, $Q = (x_2, y_2, t_2)$ et $R = (x_3, y_3, t_3)$. On calcule les coordonnées des points S, T, U, V, W, X . On remarque d'abord que, lorsqu'on a deux points $M, N \in \Gamma$ et qu'on cherche le point où (MN) recoupe Γ , les coordonnées de ce point sont rationnelles par rapport à celles de M, N (c'est un simple calcul de fonctions symétriques des racines). Quitte à multiplier par les dénominateurs, on peut même les supposer polynomiales. Les coordonnées des points de la figure

s'expriment donc comme des polynômes en les x_i, y_i, t_i et l'égalité $U = X$ s'écrit comme la nullité de plusieurs polynômes homogènes en ces variables (les 2-mineurs de la matrice 2×3 des coordonnées des deux points). Pour montrer que ces polynômes sont nuls partout, on peut plonger k dans une clôture algébrique \bar{k} . On sait alors que ces polynômes sont nuls sur l'ouvert de Zariski non vide où les points sont distincts. Comme Γ est non singulière, elle est irréductible, donc aussi $\Gamma \times \Gamma \times \Gamma$ et les polynômes sont nuls partout.

3.5.29 Remarque. Le lecteur pourra faire les calculs évoqués ci-dessus de manière explicite²¹ à partir de la cubique d'équation affine $y^2 = x^3 + ax^2 + bx + c$. Si on part de $P = (x_1, y_1)$ et $Q = (x_2, y_2)$, on montre aisément que $P \vee Q$ a pour coordonnées affines :

$$x_3 = \lambda^2 - a - x_1 - x_2, \quad y_3 = \lambda x^3 + \nu,$$

avec $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ et $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$.

3.6 Exercices

3.6.1 Une autre preuve de 3.1.1

3.6.1 Exercice. On reprend les notations de 3.1.1. On choisit comme repère a, ω, b, d où ω est le pôle de (ab) (de sorte que (ωa) et (ωb) sont tangentes à Γ) et d un point de Γ . Si on pose $a = (1, 0, 0)$, $\omega = (0, 1, 0)$, $b = (0, 0, 1)$ et $d = (1, 1, 1)$, la conique Γ a pour équation $Y^2 - XT = 0$.

Soit Δ une droite passant par a , d'équation $\lambda Y + \mu T$. Calculer successivement le point $p = \pi_a^{-1}(\Delta)$, puis l'équation de la droite $(bp) = \pi_b(p)$. Conclure.

3.6.2 Pascal et les points confondus

3.6.2 Exercice. On reprend les notations du théorème de Pascal.

1) On suppose $a = b'$ mais les autres points distincts. Montrer que la démonstration proposée s'applique sans changement, à condition de remplacer (ab') par la tangente en a .

2) On suppose $a = b'$ et $b = a'$ et on remplace les droites (ab') et $(a'b)$ par les tangentes aux points correspondants. Montrer que le théorème de

²¹Voir le livre de Silverman et Tate, *Rational points on elliptic curves*, Springer, 1992.

Pascal est encore vrai. (On pourra, par exemple, introduire les points $x = (a'c) \cap T_a$ et $y = (bc') \cap T_a$ où T_a désigne la tangente en a et montrer l'égalité $\llbracket y, x, w, a \rrbracket = \llbracket y, b, u, c' \rrbracket$.)

3) Traiter de manière analogue le cas $a = b'$ et $b = c'$.

4) On suppose $a = b'$, $b = c'$, $c = a'$. On se propose de montrer que le théorème de Pascal est encore vrai en remplaçant (ab') , (bc') et (ca') par les tangentes T_a, T_b, T_c aux points a, b, c .

a) On pose $x = T_b \cap T_c$, $y = T_c \cap T_a$, $z = T_a \cap T_b$. Montrer que les polaires de u, v, w sont respectivement (by) , (cz) et (ax) .

b) Soit o le point d'intersection de (cz) et (ax) . Montrer que o est conjugué de u par rapport à la conique. (On montrera que (oy) est la polaire de u par rapport aux droites (ya) et (yc) .)

c) En déduire que les polaires de u, v, w sont concourantes et conclure.

3.6.3 Involutions, axe d'homographie, etc.

Commutation des involutions

3.6.3 Exercice. Soit Γ une conique propre non vide, a, b deux points distincts du plan non situés sur Γ . On considère les involutions σ_a et σ_b de points de Frégier a, b .

1) Montrer que les propriétés suivantes sont équivalentes :

- i) σ_a et σ_b commutent,
- ii) le produit $\sigma_a \sigma_b$ est une involution,
- iii) σ_a fixe b ,
- iv) les points a, b sont conjugués par rapport à Γ .

(On pourra utiliser le “principe de conjugaison” : si g est une homographie, $g\sigma_a g^{-1}$ est l'involution de point de Frégier $g(a)$. Dans le cas réel, on pourra se convaincre de l'exactitude du résultat en regardant, selon les cas, les points d'intersection de (ab) et Γ et/ou celles de Γ et des polaires de a, b .)

On suppose les conditions précédentes réalisées. Soit c le pôle de (ab) . Montrer qu'on a $\sigma_a \sigma_b = \sigma_c$. (Si d est le point de Frégier de $\sigma_a \sigma_b$, la polaire de d est fixe par $\sigma_a \sigma_b$, donc contient deux des points a, b, c .)

2) Montrer que toute involution de Γ est produit de deux involutions (utiliser un triangle autopolaire). (On retrouve ici le résultat de 3.3.4 ou de 3.3.9.)

Axe d'homographie

3.6.4 Exercice. Soit Γ une conique propre, f une homographie de Γ donnée par son axe D et par l'image a' d'un point $a \in \Gamma$.

1) Construire l'image par f d'un point de D puis d'un point quelconque de $\mathbf{P}(E)$.

2) À quelle condition f est-elle une involution ?

3) Si f n'est pas une involution, montrer qu'elle est produit de deux involutions de points de Frégier $u, v \in D$ avec u arbitraire. Construire v .

3.6.5 Exercice. Soit D une droite projective réelle et f une homographie de D , donnée par trois points distincts a, b, c et leurs images a', b', c' . Construire l'image d'un point et les points fixes éventuels de f . Discuter. (On suppose le plan muni d'une droite à l'infini et d'une structure euclidienne. On considère un point s et un cercle C passant par s . L'homographie f définit une homographie f^* de s^* , puis une homographie de C , dont on construira l'axe et les points fixes.)

Cette méthode s'applique sur un corps quelconque, pourvu qu'on dispose d'une conique propre non vide.

Frégier : applications géométriques

3.6.6 Exercice. Soit D une droite projective et soit f une involution de D donnée par les images de deux points $a' = f(a)$ et $b' = f(b)$. On suppose donnée une conique Γ du plan (par exemple un cercle). Construire l'image d'un point m quelconque de D par f . (On prend un point $p \in \Gamma$ et on considère l'involution g de la droite duale p^* induite par f et les incidences. Cette involution induit une involution h de Γ dont on construit le point de Frégier.)

3.6.7 Exercice. Soit D une droite projective réelle et soit f une involution de D donnée par les images de deux points $a' = f(a)$ et $b' = f(b)$. Construire les points fixes éventuels de f . (La méthode est identique à celle de 3.6.5, à ceci près qu'une fois qu'on dispose d'une involution de Γ on a immédiatement son point de Frégier et donc ses points fixes.)

3.6.8 Exercice. Dans un plan affine euclidien on se donne une involution f d'une droite projective duale m^* par la donnée de deux droites A, B passant par m et de leurs images A', B' . Construire une droite $D \in m^*$ telle que $f(D)$ soit la perpendiculaire à D en m . (Utiliser un cercle auxiliaire Γ de centre o passant par m . Construire le point de Frégier u de l'involution induite par f sur Γ et considérer la droite (ou) .)

Frégier : applications algébriques

3.6.9 Exercice. (Centres des groupes)

On considère une conique propre non vide d'équation q .

1) Montrer que si u est un élément de $PO(q)$ et σ_a l'involution de point de Frégier a , on a $u\sigma_a u^{-1} = \sigma_{u(a)}$. En déduire que le centre de $PO(q)$ est réduit à l'identité (on pourra exhiber un repère de $\mathbf{P}(E)$ formé de points situés hors de $V(q)$).

2) ¶ On suppose $k \neq \mathbf{F}_3$.

a) Montrer que si D est une droite de $\mathbf{P}(E)$, il existe deux points distincts $a, b \in D$ tels que $q(a)q(b)$ soit un carré de k^* . (On distinguera selon que D est, ou non, une tangente, et on utilisera une base orthogonale du plan vectoriel dont l'image est D . C'est ici qu'on utilise l'hypothèse $k \neq \mathbf{F}_3$.)

b) Montrer que toute droite est l'axe d'une homographie $u \in \Omega(q)$.

c) Montrer que le centre de $\Omega(q)$ est réduit à l'identité.

d) ¶ Traiter le cas du corps \mathbf{F}_3 (attention, il n'y a que trois involutions²² dans $\Omega(q)$).

3.6.10 Exercice. (Simplicité)

On suppose que le corps k est le corps des réels et on considère une conique Γ propre non vide d'équation q . On se propose de montrer que le groupe $\Omega(q)$ est simple (c'est-à-dire qu'il n'a pas de sous-groupe distingué non trivial). On note \mathbf{K} (resp. \mathbf{T}) l'intérieur (resp. l'extérieur) de Γ . Il pourra être commode de supposer que Γ est un cercle pour une structure affine euclidienne convenable.

1) Soient a, b deux points de \mathbf{T} .

a) On suppose que (ab) coupe Γ en deux points. Montrer que $\sigma_a \sigma_b$ est produit de deux involutions de points de Frégier dans \mathbf{K} (utiliser 3.6.4).

b) On suppose que (ab) ne coupe pas Γ ou lui est tangente. Montrer que $\sigma_a \sigma_b$ est produit de quatre involutions de points de Frégier dans \mathbf{K} (choisir un point $c \in \mathbf{T}$ tel que (ac) et (bc) coupent Γ .) Montrer, réciproquement, que tout produit de quatre involutions de points de Frégier dans \mathbf{K} est une homographie dont l'axe est tangent ou extérieur à Γ .

c) En déduire que tout élément de $\Omega(q)$ est produit de 1, 2 ou 4 involutions de points de Frégier dans \mathbf{K} (donc d'involutions appartenant à $\Omega(q)$).

2) Montrer qu'une homographie de $PO(q)$ dont l'axe ne coupe pas Γ , ou lui est tangent, est dans $\Omega(q)$. (Utiliser 3.6.4.)

3) Soit N un sous-groupe distingué de $\Omega(q)$, non réduit à l'identité.

²²Le plus simple est sans doute de noter que le groupe $PO(q)$ agit fidèlement et triplement transitivement sur la conique. Comme celle-ci n'a que quatre points, ça ne laisse pas beaucoup de choix.

a) On suppose que N contient une involution. Montrer qu'il les contient toutes et conclure.

b) On suppose que N contient le produit $u = \sigma_a \sigma_b$ de deux involutions de points de Frégier distincts $a, b \in \mathbf{T}$. Soit c un point de \mathbf{K} situé sur la polaire de b . On pose $a' = \sigma_c(a)$. Montrer que (aa') coupe Γ . Montrer qu'on a $\sigma_c u \sigma_c^{-1} = \sigma_{a'} \sigma_b$. En déduire que $v = \sigma_{a'} \sigma_a$ est dans N et que v est produit de deux involutions de points de Frégier situés dans \mathbf{K} .

c) On suppose que N contient le produit u de deux involutions de points de Frégier distincts et intérieurs. Montrer que u est produit de deux involutions de points de Frégier a, b extérieurs, distincts et tels que la droite (ab) coupe Γ .

Montrer qu'il existe un point c sur la polaire de b , extérieur à Γ , tel que $e = \sigma_c(a)$ soit sur la polaire de a . (On pourra faire le calcul²³ en posant $q = Y^2 - XT$, $b = (0, 1, 0)$, $a = (x, y, t)$ et chercher c sous la forme $(\alpha, 0, \gamma)$.)

Soit d le pôle de (ab) . On pose $v = \sigma_e \sigma_d$. Montrer que v est dans Ω , qu'on a $vvv^{-1}u^{-1} = \sigma_e \sigma_a$, que cet élément est dans N et que c'est une involution.

Conclure.

Les automorphismes de $PO(q)$

3.6.11 Exercice. ¶

On suppose $k = \mathbf{R}$. Soit \bar{q} une conique propre non vide, $\Gamma = V(q)$. L'objectif de cet exercice est de déterminer les automorphismes du groupe $PO(q)$. Soit $\phi : PO(q) \rightarrow PO(q)$ un automorphisme de groupe.

1) Montrer que l'image par ϕ d'une involution de $PO(q)$ est une involution et que ϕ induit une bijection de l'ensemble des involutions sur lui-même. En déduire que ϕ induit une bijection ψ de $\mathbf{P}(E) - \Gamma$ sur lui-même définie par $\phi(\sigma_a) = \sigma_{\psi(a)}$.

2) Montrer que deux involutions distinctes σ_a et σ_b commutent si et seulement si leurs points de Frégier sont conjugués (voir 3.6.3). En déduire que, si a, b sont deux points distincts de $\mathbf{P}(E) - \Gamma$, la droite (ab) est tangente à Γ si et seulement si il n'existe pas d'involution i commutant à σ_a et σ_b et qu'alors la droite $(\psi(a)\psi(b))$ est tangente à Γ .

3) Montrer que si trois points $a, b, c \notin \Gamma$ sont alignés sur une tangente à Γ , il en est de même de leurs images par ψ (sinon, ils forment un triangle circonscrit et l'intervention d'un quatrième point de la tangente mène à une contradiction).

²³Je suis convaincu qu'on peut prouver géométriquement ce résultat. Le lecteur qui y parviendra aura gagné ma considération.

4) Montrer qu'on peut prolonger ψ en une bijection de $\mathbf{P}(E)$ tout entier de la façon suivante. Si m est un point de Γ on choisit deux points distincts a, b de la tangente en m et on associe à m le point de contact de la tangente $(\psi(a)\psi(b))$.

5) Montrer que trois points a, b, c de $\mathbf{P}(E) - \Gamma$ sont alignés sur une droite non tangente à Γ si et seulement si il existe une involution u qui commute avec σ_a, σ_b et σ_c . En déduire que ψ conserve l'alignement.

6) Montrer que ψ est une homographie (on utilisera le théorème fondamental de la géométrie projective, cf. Partie I, ??), puis que ψ est dans $PO(q)$. En déduire que ϕ est l'automorphisme intérieur associé à ψ .

3.6.4 Autour du lemme de Poncelet

3.6.12 Exercice. Dans cet exercice on traite le cas particulier du lemme de Poncelet 3.4.1.

Soit Γ une conique propre non vide et soient a et b des points non situés sur Γ , conjugués par rapport à Γ .

1) Montrer que le produit $\sigma_a \circ \sigma_b$ des involutions de points de Frégier a et b est l'involution dont le point de Frégier est le pôle e de (ab) .

2) Soit $p \in \Gamma$. Les droites (ap) et (bp) recoupent Γ en c et d . Soit m le point d'intersection des tangentes à Γ en c et d . Montrer que la polaire de m est la droite (cd) et que cette droite passe par e . En déduire que m décrit la droite (ab) .

3.6.13 Exercice. Cet exercice présente la forme originelle du lemme de Poncelet. Soient Δ_1, Δ_2 deux droites projectives et Γ une conique propre non vide. Soit p un point de Γ . La tangente T à Γ en p coupe Δ_i en a_i . Soient D_1 et D_2 les tangentes à Γ issues de a_1 et a_2 et distinctes²⁴ de T . Les droites D_1 et D_2 se coupent en m . Montrer que, lorsque p varie sur Γ , m décrit une conique. (On introduira le pôle d_i de Δ_i par rapport à Γ .)

3.6.5 Retrouver des lois de groupes sur les coniques

Dans ce paragraphe, on met en évidence l'existence de lois de groupes sur une conique privée d'un ou deux points. Comme une conique est en bijection avec une droite projective, donc avec $k \cup \{\infty\}$, on conçoit qu'on va retrouver les lois de groupe additif sur k et multiplicatif sur k^* , mais on va les décrire

²⁴Avec les conventions usuelles en cas de coïncidence des points.

de manière géométrique. Ces résultats permettront de traiter certains cas particuliers du grand théorème de Poncelet au chapitre suivant.

3.6.14 *Exercice. Le groupe multiplicatif*

Soit C une conique propre, a, b, c trois points distincts de C . Montrer qu'on définit sur $C - \{a, b\}$ une structure de groupe d'élément neutre c , isomorphe à (k^*, \times) en définissant le produit de deux éléments x, y comme l'élément z obtenu comme suit : on appelle p le point d'intersection²⁵ de (xy) et (ab) et z le second point d'intersection de C et de (cp) . (On montrera que l'application qui à x associe le birapport $[[a, b, c, x]]$ est un isomorphisme du groupe considéré sur k^* en montrant notamment l'égalité $[[a, b, c, x]] = [[b, a, z, y]]$.)

3.6.15 *Exercice. Le groupe additif* Soit C une conique propre, a, b deux points distincts de C . Montrer qu'on définit sur $C - \{a\}$ une structure de groupe d'élément neutre b , isomorphe à $(k, +)$ en définissant le produit de deux éléments x, y comme l'élément z obtenu comme suit : on appelle u le point d'intersection de (xy) et de la tangente à C en a et z est alors l'autre point d'intersection de C et de la droite (bu) . (On établira l'égalité de birapports : $[[b, a, x, z]] = [[b, y, a, z]]$.)

²⁵Avec les conventions usuelles.

Chapitre 4

L'espace des coniques

Dans ce chapitre nous étudions l'espace des coniques, autour des notions d'intersection et de pinceau de coniques. Parmi les applications, outre la résolution par radicaux des équations de degré 4, nous reviendrons sur le théorème de Pascal et sa version en termes d'invariants, nous achèverons l'étude du théorème de l'involution de Desargues et nous terminerons cette partie par l'un des plus beaux théorèmes portant sur les coniques : le grand théorème de Poncelet.

Dans tout ce chapitre E est un espace vectoriel de dimension 3 sur k et Q l'espace vectoriel des formes quadratiques sur E .

Si on choisit une base de E , on sait que Q est isomorphe à l'espace vectoriel \mathcal{S} des matrices 3×3 symétriques à coefficients dans k . C'est donc un espace de dimension 6 et l'espace $\mathbf{P}(Q)$ des coniques est un espace projectif de dimension 5. En coordonnées on écrira une conique sous la forme

$$(*) \quad q(X, Y, T) = uX^2 + vY^2 + wT^2 + 2u'YT + 2v'TX + 2w'XY.$$

4.1 Intersection de coniques

4.1.1 Coniques passant par cinq points

4.1.1 Proposition.

- 1) Par cinq points du plan passe au moins une conique.
- 2) Par cinq points du plan "en position générale" (i.e. tels que 3 quelconques ne sont pas alignés) passe une unique conique. Cette conique est propre.

Démonstration. 1) Soient $a_i = (x_i, y_i, t_i)$, $i = 1, \dots, 5$ les points donnés. On cherche les coniques sous la forme (*) ci-dessus. Cela revient à résoudre les cinq équations linéaires en les 6 inconnues u, v, w, u', v', w' suivantes :

$$ux_i^2 + vy_i^2 + wt_i^2 + 2u'y_it_i + 2v't_ix_i + 2w'x_iy_i = 0.$$

L'espace des solutions est un sous-espace vectoriel de Q de dimension ≥ 1 . Il contient donc une forme q non nulle qui donne la conique cherchée.

2) Si les cinq points a, b, c, d, e sont en position générale, les quatre premiers forment un repère et l'on peut donc supposer qu'on a $a = (1, 0, 0)$, $b = (0, 1, 0)$, $c = (0, 0, 1)$, $d = (1, 1, 1)$. On pose $e = (\alpha, \beta, \gamma)$ et l'hypothèse de position générale implique $\alpha, \beta, \gamma \neq 0$ et α, β, γ distincts. Les équations précédentes donnent alors $u = v = w = 0$, $u' + v' + w' = 0$ et $u'\beta\gamma + v'\gamma\alpha + w'\alpha\beta = 0$. Les 2-mineurs de ce système sont non nuls. Il est donc de rang 2 et admet une unique solution, à un scalaire près :

$$u' = \alpha(\beta - \gamma), \quad v' = \beta(\gamma - \alpha), \quad w' = \gamma(\alpha - \beta).$$

On voit qu'il y a une unique conique Γ solution. Pour voir qu'elle est propre il suffit de calculer le discriminant de l'équation de Γ :

$$\begin{vmatrix} 0 & \gamma(\alpha - \beta) & \beta(\gamma - \alpha) \\ \gamma(\alpha - \beta) & 0 & \alpha(\beta - \gamma) \\ \beta(\gamma - \alpha) & \alpha(\beta - \gamma) & 0 \end{vmatrix} = 2\alpha\beta\gamma(\alpha - \beta)(\beta - \gamma)(\gamma - \alpha) \neq 0.$$

4.1.2 Remarques.

1) La condition de position générale est nécessaire pour avoir une conique propre solution en vertu du "petit Bézout" 2.2.9.

2) Dans la preuve précédente, pour prouver que Γ est propre, il suffit de noter que cinq points en position générale ne peuvent être sur une conique dégénérée (considérer les trois cas d'une droite double, deux droites sécantes et un point isolé).

3) Si les points ne sont pas en position générale, plusieurs phénomènes peuvent se passer :

a) La conique peut être unique mais impropre (prendre par exemple $a = (1, 0, 0)$, $b = (0, 1, 0)$, $c = (0, 0, 1)$, $d = (1, 1, 0)$, $e = (1, 0, 1)$, l'unique conique passant par ces points est $q = YT$).

b) Il peut y avoir plusieurs solutions (prendre $a = (1, 0, 0)$, $b = (0, 1, 0)$, $c = (1, 1, 0)$, $d = (0, 0, 1)$, $e = (1, 2, 0)$, les solutions sont les coniques $q = T(\lambda X + \mu Y)$).

4) Comme une conique sur le corps \mathbf{F}_3 a exactement quatre points (elle est

en bijection avec $\mathbf{P}^1(k)$), cela montre que cinq points du plan sur \mathbf{F}_3 ne sont jamais en position générale au sens défini ci-dessus !

5) La remarque précédente montre bien que les mots “en position générale”, n’ont pas toujours un sens univoque. Traditionnellement, en géométrie algébrique, ils signifient seulement que les points a, b, c, d, e décrivent un ouvert de Zariski (voir Partie II ??) de $\mathbf{P}(E)^5$. Ainsi, dans le problème précédent il y a une autre notion : on peut dire que les points sont en position générale si les 5-mineurs du système d’équations rencontré ci-dessus sont non tous nuls, ce qui signifie exactement qu’il existe une unique conique passant par ces points. Comme les mineurs sont des polynômes en les coefficients des points, cette condition définit bien un ouvert de Zariski de $\mathbf{P}(E)^5$. Si les cinq points sont distincts, le lecteur montrera sans peine que cette condition d’unicité revient à dire qu’il n’y a pas plus de trois points alignés¹ parmi les cinq.

4.1.2 Coniques tangentes à cinq droites

La proposition 4.1.1 se traduit par dualité :

4.1.3 Corollaire.

- 1) *Il existe une conique tangente à cinq droites données.*
- 2) *Si cinq droites sont en position générale (i.e. si trois d’entre elles ne sont pas concourantes), il existe une unique conique qui leur est tangente et cette conique est propre.*

4.1.3 Le théorème de Bézout faible

4.1.4 Corollaire. (Bézout faible) *Si Γ est une conique propre et Γ' une conique quelconque, différente de Γ , on a $|\Gamma \cap \Gamma'| \leq 4$.*

Démonstration. Si $|\Gamma \cap \Gamma'|$ est > 4 , on choisit cinq points dans l’intersection. Ces points sont en position générale en vertu de 2.2.9 et cela contredit l’unicité dans 4.1.1.

Dans la figure 4.1, on trouve des exemples de coniques se coupant en 0, 1, 2 ou 4 points dans le plan réel.

4.1.5 Remarque. Voir aussi 3.5.14 pour un résultat plus général. Pour une preuve par le calcul, voir paragraphe 4.1.5 ci-dessous.

Le corollaire suivant comporte un petit piège :

¹On retrouve la condition de stabilité de cinq points au sens de Mumford, voir Partie II chapitre 7.

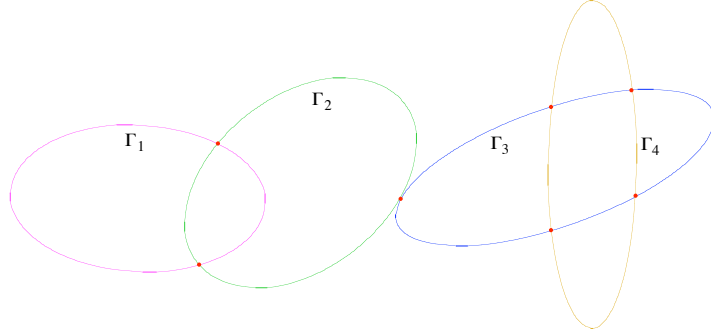


Figure 4.1: Quelques situations d'intersection de coniques.

4.1.6 Corollaire. *On suppose $k \neq \mathbf{F}_3$. Si une conique Γ' contient une conique propre non vide Γ , elle lui est égale.*

Démonstration. Le cardinal de l'intersection est au moins égal à celui de Γ donc de $\mathbf{P}^1(k)$, donc à $|k| + 1$. Comme le corps k est différent de \mathbf{F}_3 , ce cardinal est au moins égal à cinq et Bézout montre qu'on a $\Gamma = \Gamma'$.

4.1.7 Remarque. Le résultat précédent est faux sur le corps à trois éléments. Ainsi, la conique Γ d'équation $Y^2 - XT = 0$ est formée des quatre points $(0, 0, 1)$, $(1, 0, 0)$, $(1, 1, 1)$, $(-1, 1, -1)$ et elle est strictement contenue dans la réunion des droites $Y = 0$ et $X = T$.

4.1.4 Application : pinceaux homographiques de droites et coniques

Le résultat projectif

4.1.8 Théorème. *Soient m et m' deux points distincts du plan $\mathbf{P}(E)$ et $f : m^* \rightarrow (m')^*$ une homographie. Si D est une droite de m^* distincte de $D_0 = (mm')$ on a $f(D) \neq D$. Soit d le point d'intersection de D et $f(D)$.*

1) Si on a $f(D_0) = D_0$ le point d décrit, quand D varie dans $m^ - (mm')$, une droite privée d'un point.*

2) Si on a $f(D_0) \neq D_0$ le point d décrit, quand D varie dans m^ , une conique propre passant par m et m' .*

Démonstration. 1) Supposons $f(D_0) = D_0$. Soient $D_1, D_2, D_3 \in m^*$, distinctes et distinctes de D_0 et d_i l'intersection de D_i et de $f(D_i)$. Il s'agit de montrer que d_3 est sur la droite $(d_1 d_2)$. Mais, on a l'égalité $\llbracket D_0, D_1, D_2, D_3 \rrbracket = \llbracket D_0, f(D_1), f(D_2), f(D_3) \rrbracket$, d'où le résultat par Partie I ??.

2) Cette fois, on suppose $f(D_0) \neq D_0$. Soient $D_1, D_2, D_3 \in m^*$, distinctes et distinctes de (mm') et d_i l'intersection de D_i et de $f(D_i)$. Alors, les cinq points m, m', d_1, d_2, d_3 sont en position générale. En effet, m, m', d_i ne sont pas alignés car $D_i \neq D_0$, m, d_i, d_j (ou m', d_i, d_j) ne le sont pas car $D_i \neq D_j$, enfin d_1, d_2, d_3 ne sont pas alignés car sinon on aurait $f(D_0) = D_0$ en vertu de Partie I ??.

Il existe donc une unique conique Γ passant par ces cinq points et elle est propre en vertu de 4.1.1. Soit $D \in m^*$ une droite distincte des D_i et d son intersection avec $f(D)$. La droite D (resp. $f(D)$) recoupe Γ en d' (resp. d''), éventuellement confondus avec m ou m' si D ou $f(D)$ est tangente à Γ . Utilisant la définition du birapport sur la conique et l'homographie f on obtient les égalités de birapports $\llbracket d_1, d_2, d_3, d' \rrbracket = \llbracket D_1, D_2, D_3, D \rrbracket = \llbracket f(D_1), f(D_2), f(D_3), f(D) \rrbracket = \llbracket d_1, d_2, d_3, d'' \rrbracket$, ce qui montre qu'on a $d' = d'' = d$, de sorte que d est sur Γ . La réciproque est immédiate.

Notons les deux cas particuliers : si D est tangente à Γ en m , on a $f(D) = (mm')$; si $D = (mm')$, $f(D)$ est la tangente à Γ en m' .

Une application euclidienne

Anticipant un peu sur la partie V, nous proposons une application euclidienne classique du résultat précédent :

4.1.9 Corollaire. *Soit X un plan affine euclidien et soient abc un triangle et D une droite ne passant par a, b, c . Soit $p \in D$. La perpendiculaire à (ap) en a recoupe D en q . Soit d le point d'intersection de (bp) et (cq) . Lorsque p décrit D , le point d décrit une conique passant par b et c .*

Démonstration. On plonge X dans un plan projectif $\mathbf{P}(E)$ comme complémentaire d'une droite à l'infini D_∞ . En vertu de la proposition précédente, il suffit de montrer que l'application f de b^* dans c^* qui à la droite (bp) associe (cq) est une homographie. Mais, f s'obtient en composant les applications suivantes : $(bp) \mapsto p$, $p \mapsto (ap)$, $i : (ap) \mapsto (aq)$, $(aq) \mapsto q$ et enfin $q \mapsto (cq)$. Ces applications sont toutes des incidences, à l'exception de i qu'on peut encore décomposer en trois applications : l'incidence qui associe à (ap) son point à l'infini p' , puis l'involution \perp de D_∞ dans elle même qui associe à la direction p' son orthogonale $(p')^\perp = q'$ et enfin l'incidence qui à q' associe (aq') . Comme les incidences sont des homographies, ainsi que l'application \perp (cf. Partie I, ??), il en résulte que f est une homographie. On vérifie qu'elle ne fixe pas la droite (bc) (car l'application \perp n'a pas de point fixe).

4.1.10 Remarque. Bien entendu, la définition de l'homographie f nécessite de prendre en compte les cas particuliers de parallélisme. Par exemple, si

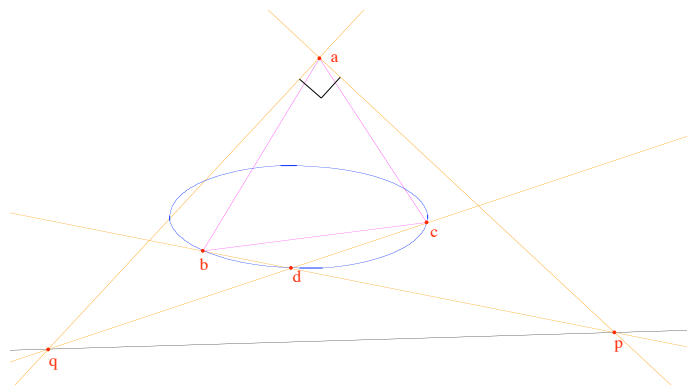


Figure 4.2: L'orthogonalité vue comme homographie.

(aq) est parallèle à D , le point q est le point à l'infini ω de D et la droite (cq) est la parallèle à D passant par c . De plus, il faut aussi définir d dans le cas $p = \omega$. Dans ce cas, les droites (ap) et (bp) sont respectivement les parallèles à D passant par a et b .

4.1.5 Multiplicités d'intersection

Dans ce paragraphe on définit la multiplicité d'intersection de deux coniques en un point. Le problème général de définir et de calculer la multiplicité d'intersection de deux variétés algébriques est un des problèmes majeurs de la géométrie algébrique (voir [Per95], [Ful69], [Ful84], etc.) et il ne saurait être question de l'aborder ici. On a donc choisi une approche très élémentaire, utilisant le paramétrage des coniques, à la manière de [Ber90]. Le défaut de cette approche c'est qu'elle ne se généralise pas aux courbes de degré > 2 .

Définition

Dans tout ce paragraphe, on suppose que le corps k n'est pas le corps \mathbf{F}_3 .

Reprenons la situation du théorème de Bézout faible 4.1.4 On considère deux coniques \bar{q} et \bar{q}' distinctes et on suppose que \bar{q} est propre. On pose $\Gamma = V(q)$ et $\Gamma' = V(q')$. On sait que Γ n'est pas contenue dans Γ' (cf. 4.1.6). Quitte à faire une homographie, on peut supposer qu'on a $q = Y^2 - XT$ et que le point $\omega = (1, 0, 0)$ de Γ n'est pas sur Γ' . On suppose que q' est de la forme $(*)$ du début de ce chapitre. En vertu de 3.1.6, on peut écrire tous les points de Γ sous la forme $(\lambda^2, \lambda\mu, \mu^2)$ avec λ, μ non tous deux nuls. Les points d'intersection de Γ et Γ' sont donnés par l'équation $q'(\lambda^2, \lambda\mu, \mu^2)$ et, comme

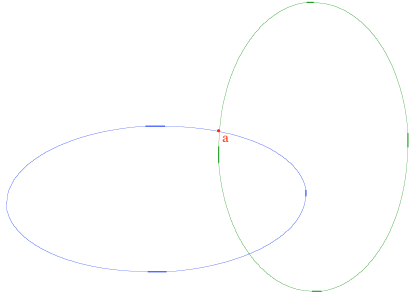


Figure 4.3: Multiplicité égale à 1

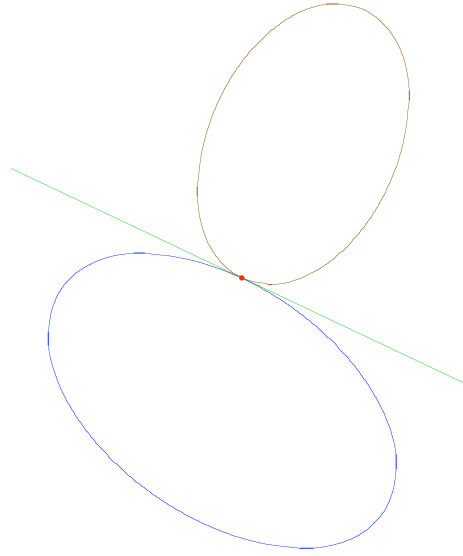


Figure 4.4: Multiplicité égale à 2

ω n'est pas sur Γ' , on peut même supposer $\mu = 1$. Il reste alors l'équation suivante :

$$(**) \quad P(\lambda) = u\lambda^4 + v\lambda^2 + w + 2u'\lambda + 2v'\lambda^2 + 2w'\lambda^3 = 0.$$

Cette équation n'est pas triviale (i.e. ses coefficients ne sont pas tous nuls). En effet, sinon, on aurait $u = w = u' = w' = 0$ et $v = -2v'$ et q' serait proportionnelle à q , ce qui est absurde puisque les coniques associées sont distinctes. L'équation $(**)$ a donc au plus 4 racines et on retrouve le résultat de 4.1.4. De plus, on peut alors définir :

4.1.11 Définition. Soit $m = (\lambda^2, \lambda, 1)$ un point de Γ . La **multiplicité d'intersection** de q et q' en m est la multiplicité de λ comme racine du polynôme $P(X)$. On la note $\mu(m, \Gamma \cap \Gamma')$. Cette multiplicité est comprise entre 0 et 4. Elle est nulle si les coniques ne se coupent pas en m . Si μ est > 0 , on dit respectivement que les coniques sont **transverses**, **tangentes**, **osculatrices** et **surosculatrices** en m selon que μ est égal à 1, 2, 3 ou 4.

Variantes de Bézout

Avec cette notion, on a une nouvelle variante de Bézout :

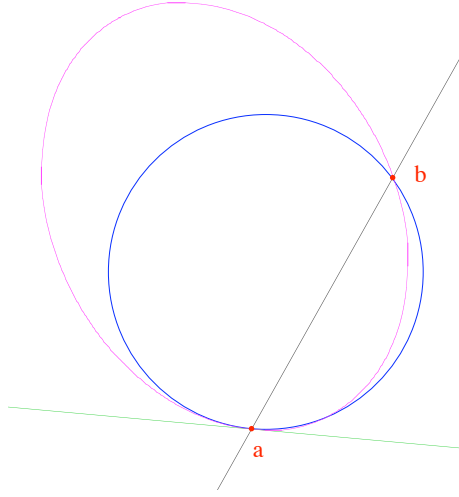


Figure 4.5: Multiplicité égale à 3

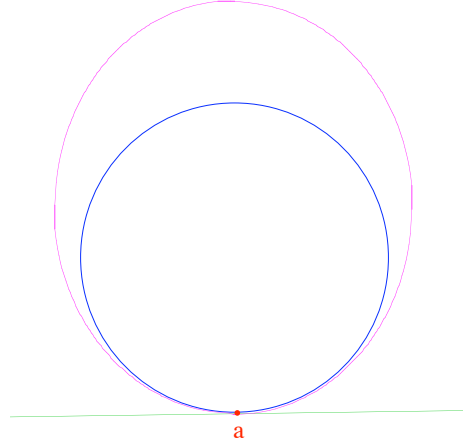


Figure 4.6: Multiplicité égale à 4

4.1.12 Proposition. (Bézout moyen) Soit Γ une conique propre et Γ' une conique distincte de Γ . On a $\sum_{m \in \mathbf{P}(E)} \mu(m, \Gamma \cap \Gamma') \leq 4$.

Démonstration. En effet, le polynôme P admet au plus 4 racines comptées avec leurs multiplicités.

Enfin, si le corps est algébriquement clos :

4.1.13 Proposition. (Bézout fort) On suppose le corps k algébriquement clos. Soit Γ une conique propre et Γ' une conique distincte de Γ . On a $\sum_{m \in \mathbf{P}(E)} \mu(m, \Gamma \cap \Gamma') = 4$.

Démonstration. C'est le fait que k est algébriquement clos².

Interprétation géométrique de la multiplicité d'intersection

4.1.14 Proposition. On suppose que les coniques Γ et Γ' sont propres, distinctes, et se coupent en m .

- 1) On a $\mu(m, \Gamma \cap \Gamma') \geq 2$ si et seulement si les coniques ont même tangente en m .
- 2) On suppose $\mu := \mu(m, \Gamma \cap \Gamma') \geq 2$.
 - a) Si Γ et Γ' se coupent en deux points a, b distincts autres que m , on a $\mu = 2$.

²Sur \mathbf{C} on parlerait du théorème de D'Alembert.

b) Si Γ et Γ' se coupent en un unique point a distinct de m , on a $\mu = 2$ si elles ont même tangente en a et $\mu = 3$ sinon.

c) Si Γ et Γ' n'ont aucun autre point d'intersection que m on a $\mu = 2$ ou 4 . Si la tangente en m a pour équation $l = 0$, les coniques sont surosculatrices si et seulement si on a $q' = \alpha q + \beta l^2$ avec $\beta \neq 0$.

Démonstration. 1) On reprend les notations du début du paragraphe 4.1.5. On peut supposer, de plus, que m est le point $(0, 0, 1)$ correspondant au paramètre $\lambda = 0$ sur Γ . La tangente à Γ (resp. Γ') en m est la droite d'équation $X = 0$ (resp. $u'Y + v'X = 0$) (voir 2.2.17). Dire qu'on a $\mu \geq 2$ c'est dire que u' est nul c'est-à-dire que les tangentes sont égales.

2) Les points a) et b) viennent du théorème de Bézout “moyen”. (Dans le cas de b) on doit noter que si P admet trois racines dans le corps il en a quatre.) Pour l'assertion complémentaire du c) il suffit de regarder les équations dans le cas $m = (0, 0, 1)$: le cas d'osculation correspond à $v + 2v' = 0$, la surosculation impose de plus $w' = 0$.

4.1.15 Remarques.

1) Sur un corps k quelconque, on n'a pas de bonne condition géométrique pour départager les coniques tangentes qui ne se recoupent pas et les surosculatrices, voir cependant ci-dessous une caractérisation en termes de pinceau. Bien entendu, si les coniques sont tangentes elles se coupent en deux autres points pourvu qu'on fasse une extension quadratique du corps. On notera que ce cas ne peut donc pas se produire si le corps est algébriquement clos. Si k est le corps des réels on a une caractérisation en termes de courbure (les courbures sont égales si et seulement si les coniques sont osculatrices).

2) Si Γ' est dégénérée en deux droites sécantes en a , on vérifie facilement les faits suivants :

- $\mu := \mu(m, \Gamma \cap \Gamma') = 1$ si $m \neq a$ et si la droite D contenue dans Γ' et passant par m n'est pas tangente à Γ ,
- $\mu = 2$ si $m \neq a$ et si D est tangente à Γ ou si $m = a$ et si les droites contenues dans Γ' ne sont pas tangentes à Γ ,
- $\mu = 3$ si $m = a$ et si l'une des droites est tangente.

3) Si Γ' est une droite double, la multiplicité vaut 4 ou 2 selon que cette droite est, ou non, tangente à Γ .

4) Nous laissons au lecteur le soin de définir la multiplicité d'intersection de deux coniques dégénérées en un point de manière à étendre à ces coniques les théorèmes de Bézout “moyen” et “fort”.

4.1.16 Corollaire. La multiplicité d'intersection est symétrique en Γ et Γ' .

Démonstration. Cela résulte de la proposition précédente.

Le diviseur $\Gamma \cap \Gamma'$

On donne ici une écriture commode pour décrire l'intersection de deux coniques. Pour des précisions sur la notion de diviseur, voir [Ful69], [Har77], [Per95], etc.

4.1.17 Définition. Soient Γ et Γ' deux coniques³ sans composante commune. On appelle **diviseur** $\Gamma \cap \Gamma'$ l'ensemble des points d'intersection de Γ et Γ' , affectés des multiplicités d'intersection. On écrira, de manière formelle⁴, $\Gamma \cap \Gamma' = \sum_i \mu_i m_i$ si les m_i sont les points d'intersection et les μ_i les multiplicités. Le **degré** de ce diviseur est, par définition, la somme des μ_i .

4.1.18 Remarque. Les diviseurs possibles pour l'intersection de deux coniques sont les suivants :

- Diviseurs de degré 4 : $a + b + c + d$, $2a + b + c$, $2a + 2b$, $3a + b$, $4a$. Sur un corps algébriquement clos, le théorème de Bézout fort montre que le diviseur est nécessairement de degré 4.
- Diviseurs de degré 2, $a + b$, $2a$.
- Diviseur de degré 1, a . On notera que sur \mathbf{R} , ce cas ne peut pas se produire (si un polynôme de degré 4 admet une racine réelle simple, il en a au moins deux).
- Diviseur de degré 0 : le vide.

4.2 Pinceaux de coniques

Nous abordons maintenant la notion de pinceau de coniques. Il s'agit d'un vaste sujet sur lequel existe une littérature abondante (mais souvent un peu ancienne). Une excellente référence sur ces notions est le livre [Ber90]. On suppose toujours $k \neq \mathbf{F}_3$.

4.2.1 Définition

4.2.1 Définition. On appelle **pinceau**⁵ de coniques une droite \mathcal{P} de l'espace projectif $\mathbf{P}(Q)$. Si Γ, C sont deux coniques distinctes de \mathcal{P} , on note $\mathcal{P} = (\Gamma, C)$.

³Si le lecteur n'a pas fait le travail proposé ci-dessus, il supposera par exemple que Γ est propre.

⁴Plus généralement, un diviseur sur une courbe est une combinaison linéaire formelle des points de la courbe, à coefficients entiers.

⁵On dit aussi – et surtout on disait autrefois – *faisceau* de coniques. Le mot faisceau ayant pris depuis une cinquantaine d'année un autre sens, notamment en géométrie algébrique, j'ai préféré utiliser le mot pinceau qui est sans ambiguïté.

4.2.2 Remarque. Un pinceau \mathcal{P} est donc l'image d'un plan vectoriel P de Q . Il est défini par une base quelconque de P , c'est-à-dire par deux coniques distinctes $\Gamma = V(q)$ et $\Gamma' = V(q')$ et les coniques du pinceau ont pour équations $\lambda q + \lambda' q' = 0$ avec λ et λ' non tous deux nuls.

4.2.3 Exemple. L'exemple le plus important de pinceau de coniques est obtenu en prenant un repère projectif a, b, c, d et l'ensemble des coniques passant par ces points, voir 4.2.7 ci-dessous.

Coniques dégénérées d'un pinceau

4.2.4 Proposition. Soit \mathcal{P} un pinceau défini par deux coniques $\Gamma = V(q)$ et $\Gamma' = V(q')$ distinctes.

- 1) Les coniques du pinceau sont toutes dégénérées dans cinq cas :
 - a) Γ et Γ' sont réunions de deux droites, l'une d'elles étant commune, ou toutes passant par un même point,
 - b) Γ est une droite double et Γ' est réunion de deux droites qui se coupent sur Γ , ou l'inverse,
 - c) Γ et Γ' sont toutes deux des coniques réduites à un même point,
 - d) Γ est une droite double et Γ' une conique réduite à un point et ce point est situé sur Γ , ou l'inverse,
 - e) Γ et Γ' sont deux droites doubles.
- On dit alors que le pinceau est **dégénéré**.
- 2) Si le pinceau est non dégénéré, il contient au plus trois coniques dégénérées.

Démonstration. 1) Le pinceau \mathcal{P} est engendré par deux coniques dégénérées Γ, Γ' d'équations q, q' . On distingue cinq cas.

a) Supposons que les coniques soient réunions de deux droites. On peut écrire leurs équations sous la forme $q = fg, q' = f'g'$ où f, g, f', g' sont des formes linéaires. Si toutes ces droites ont un point commun, disons $(0, 0, 1)$, leurs équations sont toutes de la forme $aX + bY = 0$ et les équations des coniques ne comportent pas de termes en T , donc sont dégénérées. Si l'une des droites est commune à Γ et Γ' , on peut supposer, par exemple, $f' = f$, toutes les coniques du pinceau contiennent la droite $f = 0$, donc sont dégénérées. Si ces conditions ne sont pas remplies, supposons que la droite d'équation f' ne passe pas par le point d'intersection de f et g . En choisissant convenablement la base de E^* , on peut supposer $f = X, g = Y, f' = T$ et $g' = aX + bY + cT$. On a alors : $\lambda fg + f'g' = \lambda XY + aXT + bYT + cT^2$. Le discriminant de cette forme est égal à $\lambda(ab - \lambda c)/4$ et il n'est nul pour tout λ que si l'on a $c = ab = 0$, autrement dit, si g' est proportionnelle à f ou g ce qui est exclu. Il y a donc une conique non dégénérée dans le pinceau.

b) Supposons que Γ est une droite double et Γ' une réunion de deux droites. On peut supposer $f = g = X$, $f' = T$ et $g' = aX + bY + cT$, avec a, b non tous deux nuls. Le discriminant de $\lambda q + q'$ est alors égal à $-\lambda b^2/4$ et il est nul pour tout λ si et seulement si on a $b = 0$, c'est-à-dire si le point double de Γ' est sur Γ .

c) Pour traiter les cas c) et d) on note que si on a deux coniques q, q' telles que toutes les coniques du pinceau engendré soient dégénérées sur le corps k , il en est de même sur n'importe quelle extension k' de k . En effet, les coniques dégénérées du pinceau différentes de q sont données par l'équation $\det(\lambda q + q') = 0$. Cette équation est à coefficients dans k et dire que toutes les coniques du pinceau sont dégénérées c'est dire que ces coefficients sont tous nuls⁶. Mais alors, l'équation est aussi triviale sur l'extension k' .

Cela permet, quitte à faire une extension quadratique, de remplacer les coniques réduites à un point par des réunions de deux droites. La conclusion vient alors de a) et b), le cas d'une droite commune aux deux pincesaux étant ici impossible (car cette droite serait à coefficients dans k).

e) Si Γ et Γ' sont toutes deux des droites doubles il est clair que toutes les coniques du pinceau sont dégénérées (prendre $q = X^2$ et $q' = Y^2$).

2) Si le pinceau n'est pas dégénéré on peut supposer que q ne l'est pas et l'équation qui donne les coniques dégénérées est $\det(\lambda q + q') = 0$. Il s'agit d'une équation de degré ≤ 3 en λ , non triviale car son coefficient dominant est $\det q$, qui admet donc au plus trois racines.

4.2.5 Remarque. Comme on a supposé $k \neq \mathbf{F}_3$, un pinceau non dégénéré contient au moins deux coniques propres distinctes. En effet, un pinceau est une droite projective, donc son cardinal est égal à $|k| + 1 \geq 6$ et il y a au plus trois coniques dégénérées. On notera que le résultat est faux sur le corps \mathbf{F}_3 comme le montre l'exemple du pinceau de base $Y(X - T)$, $(Y - T)(X + Y)$ qui ne contient qu'une conique propre : $Y^2 - XT$.

Diviseur associé à un pinceau

4.2.6 Proposition. Soit \mathcal{P} un pinceau non dégénéré défini par deux coniques propres $\Gamma = V(q)$ et $\Gamma' = V(q')$ distinctes. Le diviseur $\Gamma \cap \Gamma'$ est indépendant du choix des coniques de base. On l'appelle **diviseur associé** au pinceau \mathcal{P} .

Démonstration. Si on change, par exemple, Γ' en Γ'' d'équation $q' + \alpha q$, on voit que les points d'intersection de Γ et Γ' sont encore donnés par l'équation $q'(\lambda^2, \lambda\mu, \mu^2) = 0$. Ce sont donc les mêmes que ceux de $\Gamma \cap \Gamma'$ et avec les mêmes multiplicités.

⁶Car le corps a plus que 3 éléments!

Diviseurs associés et coniques impropres

Le lien entre coniques impropres d'un faisceau et diviseur associé est donné par la proposition suivante :

4.2.7 Proposition-Définition. *Soit \mathcal{P} un pinceau non dégénéré de coniques et soient $\Gamma = V(q)$ et $\Gamma' = V(q')$ deux coniques propres définissant \mathcal{P} . On suppose que $\Gamma \cap \Gamma'$ est de degré 4.*

1) *Si on a $\Gamma \cap \Gamma' = a + b + c + d$, les points a, b, c, d forment un repère de $\mathbf{P}(E)$, le pinceau \mathcal{P} est l'ensemble des coniques passant par ces points et il contient trois coniques dégénérées : $(ab) \cup (cd)$, $(ac) \cup (bd)$ et $(ad) \cup (bc)$. On dit que le pinceau est de type **transverse**.*

2) *Si on a $\Gamma \cap \Gamma' = 2a + b + c$ (coniques tangentes en a et transverses en b et c), on note D la tangente commune à Γ et Γ' en a . Alors, les points a, b, c sont non alignés, la droite D ne passe pas par b et c , le pinceau \mathcal{P} est l'ensemble des coniques passant par a, b, c et tangentes à D en a . Il contient deux coniques dégénérées : $(ab) \cup (ac)$ et $(bc) \cup D$. On dit que le pinceau est de type **tangent**.*

3) *Si on a $\Gamma \cap \Gamma' = 2a + 2b$ (coniques bitangentes en a et b), et si on note D_a et D_b les tangentes communes à Γ et Γ' en a et b , le pinceau \mathcal{P} est l'ensemble des coniques tangentes à D_a et D_b en a et b respectivement. Il contient deux coniques dégénérées : la droite (ab) double et la réunion des droites D_a et D_b . On dit que le pinceau est de type **bitangent**.*

4) *Si on a $\Gamma \cap \Gamma' = 3a + b$ (coniques osculatrices en a), \mathcal{P} contient une conique dégénérée, réunion de (ab) et de la tangente commune en a . On dit que le pinceau est de type **osculateur**.*

5) *Si on a $\Gamma \cap \Gamma' = 4a$ (coniques surosculatrices en a), \mathcal{P} contient une conique dégénérée, la tangente commune double. On dit que le pinceau est de type **surosculateur**.*

Démonstration. 1) Les points forment un repère car trois points distincts d'une conique propre ne sont jamais alignés. Il est clair que toutes les coniques du pinceau passent par a, b, c, d . Réciproquement, si on prend $a = (1, 0, 0)$, $b = (0, 1, 0)$, $c = (0, 0, 1)$ et $d = (1, 1, 1)$, on voit que les coniques passant par les quatre points ont pour équations $u'YT + v'TX + w'XY$ avec $u' + v' + w' = 0$. On obtient donc ainsi un plan vectoriel de Q , nécessairement égal à celui qui définit \mathcal{P} . Les réunions des droites sont alors des coniques dégénérées de \mathcal{P} et il n'y en a pas d'autres en vertu de 4.2.4.

2) La preuve est analogue. On prend $a = (1, 0, 0)$, $b = (0, 1, 0)$, $c = (0, 0, 1)$ et D d'équation $Y + T = 0$. Les coniques du pinceau ont pour équations $u'YT + v'TX + w'XY$ avec $v' = w'$. Les coniques dégénérées sont données par $u' = 0$ ou $v' = 0$ et ce sont bien celles annoncées.

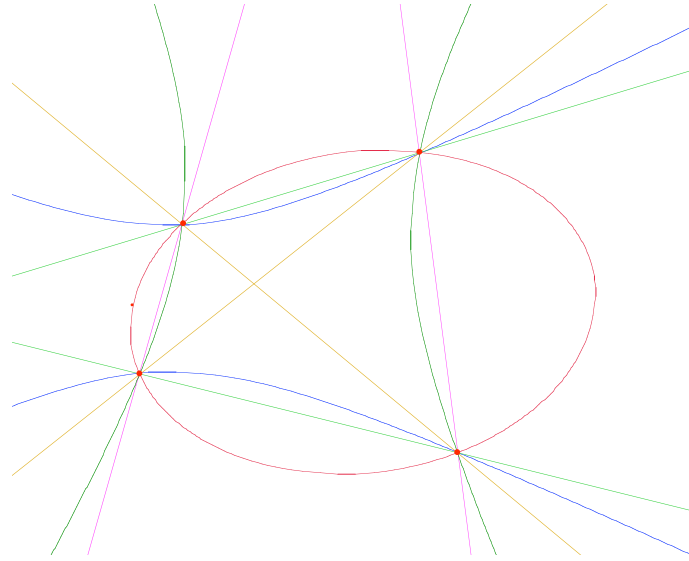


Figure 4.7: Le pinceau des coniques passant par 4 points.

3) On prend $a = (1, 0, 0)$, $b = (0, 1, 0)$, $D_a = V(Y)$, $D_b = V(X)$. On obtient les équations $wT^2 + 2w'XY = 0$ et les coniques dégénérées du pinceau sont données par $w = 0$ ou $w' = 0$.

4) On prend $a = (1, 0, 0)$, $b = (0, 0, 1)$ et $q = Y^2 - XT$. Les équations des coniques tangentes en a à Γ et passant par b sont données par $vY^2 + 2u'YT + 2v'TX = 0$. L'intersection d'une telle conique avec Γ est donnée par $T = 0$ et $(v + 2v')X + 2u'Y = 0$. La deuxième droite coupe Γ en a et b si et seulement si on a $v + 2v' = 0$. Les coniques osculatrices à Γ en a ont donc pour équations $u'YT + v(Y^2 - XT) = 0$. On voit que l'unique conique dégénérée de ce pinceau est d'équation YT .

5) On prend $a = (1, 0, 0)$ et $q = Y^2 - XT$. Un calcul facile montre que les coniques surosculatrices à Γ en a ont pour équations $wT^2 + v(Y^2 - XT) = 0$ et l'unique conique dégénérée de ce pinceau est $T^2 = 0$.

4.2.8 Remarques.

1) Comme un pinceau est déterminé par deux coniques distinctes, il est clair que, dans les cas 1), 2) et 3), les coniques dégénérées déterminent le pinceau. Cela ne subsiste pas dans les deux derniers cas.

2) Si le diviseur $\Gamma \cap \Gamma'$ est incomplet (c'est-à-dire de degré < 4), les choses sont plus compliquées, voir exercice 4.6.7 pour l'étude du cas réel.

4.2.9 Remarque. La configuration du pinceau transverse donne une interprétation de la “relation à 5 points” vue dans la Partie II ???. À permutation près, il

s'agit de la relation :

$$[b, c, m][a, d, m] - [a, c, m][b, d, m] + [a, b, m][c, d, m] = 0.$$

Cette relation exprime le fait que la conique dégénérée $(ac) \cup (bd)$, d'équation $[a, c, m][b, d, m] = 0$ est dans le pinceau défini par les coniques $(ab) \cup (cd)$ et $(ad) \cup (bc)$.

4.2.2 Classification des pinceaux

Le groupe $PGL(E)$ des homographies de $\mathcal{P}(E)$ opère sur l'espace $\mathbf{P}(Q)$ des coniques et donc aussi sur les pinceaux. Une question essentielle est celle de leur classification : étant donnés deux pinceaux \mathcal{P} et \mathcal{P}' , à quelle condition existe-t-il une homographie f qui envoie \mathcal{P} sur \mathcal{P}' ? Déjà, on a des conditions nécessaires évidentes :

4.2.10 Proposition. *Si deux pinceaux non dégénérés \mathcal{P} et \mathcal{P}' sont échangés par une homographie f , les diviseurs associés sont de même nature, les coniques impropres des pinceaux sont en même nombre et de même type.*

4.2.11 Théorème. *Soient \mathcal{P} et \mathcal{P}' deux pinceaux non dégénérés. On suppose que les diviseurs associés sont tous deux de degré 4. Les pinceaux \mathcal{P} et \mathcal{P}' sont dans la même orbite sous l'action du groupe $PGL(E)$ si et seulement s'ils sont de même type⁷ (c'est-à-dire tous deux transverses ou tangents ou bitangents ou osculateurs ou surosculateurs).*

Démonstration. On notera que dans les trois premiers cas les pinceaux contiennent au moins deux coniques dégénérées, de sorte que ces coniques les déterminent.

Si \mathcal{P} et \mathcal{P}' sont transverses, leurs diviseurs respectifs sont $a + b + c + d$ et $a' + b' + c' + d'$, ces points formant des repères de $\mathbf{P}(E)$. Il existe alors une homographie qui envoie a, b, c, d sur a', b', c', d' . Elle envoie aussi les coniques dégénérées de \mathcal{P} sur celles de \mathcal{P}' , donc \mathcal{P} sur \mathcal{P}' .

Si les pinceaux sont tangents, notons respectivement $2a + b + c$ et $2a' + b' + c'$ leur diviseurs et D et D' les tangentes communes en a et a' . On choisit un point d (resp. d') sur D (resp. D'), non situé sur (bc) (resp. $(b'c')$). Alors l'homographie qui envoie a, b, c, d sur a', b', c', d' convient.

Si les pinceaux sont bitangents en a, b et a', b' respectivement et si les tangentes communes sont D_a, D_b et $D_{a'}, D_{b'}$ il suffit de choisir des points c, d, c', d' sur les tangentes et la conclusion s'ensuit de manière analogue.

⁷Sauf erreur de ma part, Berger [Ber90] est inutilement prudent ici.

Dans les deux derniers cas, le pinceau contient au moins une conique propre (voir 4.2.5), non vide puisque le diviseur du pinceau est de degré 4. Comme le groupe $PGL(E)$ est transitif sur les coniques propres non vides en vertu de 2.2.26, on se ramène au cas où les deux pinceaux ont en commun une telle conique Γ d'équation q .

Supposons que les pinceaux soient osculateurs. Leurs diviseurs respectifs sont $3a+b$ et $3a'+b'$ avec $a, b, a', b' \in \Gamma$. Mais, le groupe $PO(q)$ est triplement transitif sur Γ (cf. 3.2.4), de sorte qu'il existe $g \in PO(q)$ qui envoie a sur a' (donc aussi la tangente D à Γ en a sur la tangente D' à Γ en a') et b sur b' . Mais alors g conserve Γ et transforme $D \cup (ab)$ en $D' \cup (a'b')$, donc \mathcal{P} en \mathcal{P}' .

Dans le cas surosculateur, les diviseurs sont $4a$ et $4a'$ avec des tangentes D et D' et on a un élément de $PO(q)$ qui envoie a sur a' , donc D sur D' . On conclut en notant que \mathcal{P} (resp. \mathcal{P}') est engendré par Γ et D^2 (resp. $(D')^2$).

4.2.12 Remarque. Pour le cas des diviseurs incomplets, voir exercice 4.6.7 dans le cas réel.

4.2.3 Classification des couples de coniques

La question, qui prendra toute son importance dans l'étude du grand théorème de Poncelet, est l'existence d'une homographie qui envoie deux coniques Γ et C sur deux autres Γ' et C' . Bien entendu, s'il existe une telle homographie, les pinceaux engendrés sont échangés, donc de même type, mais il y a une condition supplémentaire. Voici le résultat dans le cas transverse :

4.2.13 Théorème. Soient Γ, C , (resp. Γ', C') deux coniques propres non vides. On suppose que les pinceaux (Γ, C) et (Γ', C') sont transverses et on note $\Gamma \cap C = \{a, b, c, d\}$ et $\Gamma' \cap C' = \{a', b', c', d'\}$. Il existe une homographie u telle que $u(\Gamma) = \Gamma'$ et $u(C) = C'$ si et seulement s'il existe une permutation σ de a', b', c', d' telle que l'on ait :

$$[a, b, c, d]_{\Gamma} = [\sigma(a'), \sigma(b'), \sigma(c'), \sigma(d')]_{\Gamma'} \text{ et } [a, b, c, d]_C = [\sigma(a'), \sigma(b'), \sigma(c'), \sigma(d')]_{C'}$$

où l'indice désigne la conique sur laquelle est pris le birapport.

Démonstration. Supposons qu'il existe une homographie convenable. Elle envoie l'ensemble $\{a, b, c, d\}$ sur $\{a', b', c', d'\}$. On pose $\sigma(x') = u(x)$ pour $x = a, b, c, d$. Comme les homographies conservent le birapport, on a le résultat.

Inversement, si on a les égalités de birapports, on peut supposer $\sigma = \text{Id}$, quitte à changer le nom des points a', b', c', d' . Il existe une homographie envoyant Γ sur Γ' . De plus, quitte à composer par une homographie de Γ' ,

on peut supposer que a, b, c s'envoient sur a', b', c' . Par conservation du birapport, le point d s'envoie aussi sur d' . Si C'' est l'image de C par u , elle contient les points a', b', c', d' et l'hypothèse et le sens direct donnent $\llbracket a', b', c'; d' \rrbracket_{C'} = \llbracket a', b', c'; d' \rrbracket_{C''}$. On conclut grâce au lemme suivant :

4.2.14 Lemme. *Soient C' et C'' deux coniques propres se coupant en quatre points a, b, c, d distincts. On suppose qu'on a $\llbracket a, b, c, d \rrbracket_{C'} = \llbracket a, b, c, d \rrbracket_{C''}$. Alors, on a $C' = C''$.*

Démonstration. Soit T'_a (resp. T''_a) la tangente à C' (resp. C'') en a . Par définition du birapport sur une conique (dans le cas limite), on a l'égalité de birapports : $\llbracket T'_a, (ab), (ac), (ad) \rrbracket = \llbracket T''_a, (ab), (ac), (ad) \rrbracket$. Cela montre que les tangentes en a sont les mêmes, donc aussi les coniques (voir 4.6.1).

4.2.15 Remarque. On peut paraphraser 4.2.13 en disant que l'invariant qui mesure l'obstruction à la transitivité du groupe $PGL(E)$ sur les couples de coniques (Γ, C) est, à permutation près, le double birapport :

$$(\llbracket a, b, c, d \rrbracket_G, \llbracket a, b, c, d \rrbracket_C)$$

de leurs points d'intersection.

4.2.4 Application à la résolution par radicaux des équations algébriques

Quelques rappels

Si k est un corps, on sait résoudre "par radicaux" les équations algébriques $P(x) = 0$, avec $P \in k[X]$, lorsque le polynôme est de degré assez petit :

- En degré 1, $P(X) = aX + b$ avec $a \neq 0$, l'unique racine est $x = -b/a$.
- En degré 2, $P(X) = aX^2 + bX + c$ avec $a \neq 0$, les racines sont $x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ (éventuellement dans une extension quadratique de k), si toutefois k n'est pas de caractéristique 2.

- En degré 3, on sait résoudre l'équation $ax^3 + bx^2 + cx + d = 0$ par la méthode dite de Cardan, initiée par les algébristes de la Renaissance italienne (Cardan, Scipion del Ferro, Tartaglia, ...). On commence par faire la translation $x' = x + \frac{b}{3a}$ (au moins si le corps n'est pas de caractéristique 3). On se ramène ainsi à une équation sans terme en x^2 : $x^3 + px + q = 0$. La méthode consiste alors à chercher x sous la forme $x = u + v$ en imposant la condition supplémentaire $3uv + p = 0$. On trouve que u^3 et v^3 vérifient $u^3 + v^3 = -q$ et $u^3v^3 = -\frac{p^3}{27}$ donc sont les racines de $y^2 + qy - \frac{p^3}{27} = 0$. On

en déduit u et v en extrayant des racines cubiques (et en tenant compte de la relation $3uv + p = 0$), puis x . Il peut être nécessaire de faire une extension de k de degré ≤ 6 . On trouve :

$$x = \sqrt[3]{-\frac{q}{2} + \frac{\sqrt{4p^3 + 27q^2}}{6\sqrt{3}}} + \sqrt[3]{-\frac{q}{2} - \frac{\sqrt{4p^3 + 27q^2}}{6\sqrt{3}}}.$$

Le degré 4

Dans la foulée de Cardan, l'un de ses élèves, Ferrari, proposa une méthode pour résoudre l'équation de degré 4 en la ramenant à une équation de degré 3 et deux de degré 2. Cette méthode se comprend mieux en utilisant les pinceaux de coniques. La situation est la suivante. Soit $P(x) = 0$ une équation de degré 4 à coefficients dans k , $P(x) = x^4 + ux^3 + ax^2 + bx + c$. Quitte à faire une translation sur la variable, on peut supposer $u = 0$. On suppose que cette équation, dans une extension algébrique convenable de k , admet 4 racines distinctes et on l'interprète comme l'équation aux x de l'intersection de deux coniques affines, l'une d'équation $f(x, y) = y - x^2 = 0$ et l'autre (par exemple⁸) $g(x, y) = y^2 + ay + bx + c = 0$. On note \bar{f} et \bar{g} les polynômes homogènes en X, Y, T associés à f et g :

$$\bar{f}(X, Y, T) = YT - X^2 \quad \text{et} \quad \bar{g}(X, Y, T) = Y^2 + aYT + bXT + cT^2$$

et \mathcal{P} le pinceau de coniques engendré par \bar{f} et \bar{g} . Comme les racines de P sont distinctes, ces coniques ont exactement 4 points en commun, de sorte que \mathcal{P} contient 3 coniques dégénérées, qui sont données par l'équation en λ , $\det(\lambda\bar{f} + \bar{g}) = 0$, équation qui est de degré 3, précisément :

$$\lambda^3 + 2a\lambda^2 + (a^2 - 4c)\lambda - b^2 = 0.$$

Cette équation est donc résoluble par la méthode de Cardan.

Si λ est l'une des racines, on considère la conique d'équation $\lambda\bar{f} + \bar{g}$, elle est dégénérée, donc décomposée en deux droites D_1, D_2 (quitte à faire une extension quadratique), que l'on peut calculer, par exemple par la méthode de Gauss de décomposition en carrés des formes quadratiques. Il ne reste plus qu'à chercher les intersections de $V(\bar{f})$ avec chacune des D_i (donc à résoudre deux équations de degré 2) et on a gagné.

⁸Un autre choix possible est $y^2 + ax^2 + bx + c$.

Un exemple

L'exemple ci-dessous est truqué pour que les calculs soient faciles. Il s'agit de résoudre l'équation : $x^4 - \frac{3}{2}x^2 + 2x - \frac{3}{16} = 0$. On a donc $a = -\frac{3}{2}$, $b = 2$ et $c = -\frac{3}{16}$. L'étude de la fonction montre que cette équation admet deux racines réelles et deux racines complexes conjuguées. On considère cette équation, comme expliqué ci-dessus, comme l'équation aux x d'intersection des coniques d'équations $y = x^2$ et $y^2 - \frac{3}{2}y + 2x - \frac{3}{16} = 0$. Les coniques dégénérées du pinceau sont données par l'équation en λ : $\lambda^3 - 3\lambda^2 + 3\lambda - 4 = 0$. Cette équation s'écrit encore $(\lambda - 1)^3 = 3$ (c'est là qu'intervient le trucage !) et donne donc $\lambda = 1 + \sqrt[3]{3}$. On choisit par exemple la racine cubique réelle et on décompose en carrés la forme quadratique (affine) associée :

$$Y^2 - \frac{3}{2}Y + 2X - \frac{3}{16} + \lambda(Y - X^2) = \left(Y + \frac{\lambda}{2} - \frac{3}{4}\right)^2 - \lambda\left(X - \frac{1}{\lambda}\right)^2$$

(on n'oubliera pas la relation qui définit λ). On obtient ainsi deux droites d'équations :

$$Y - \sqrt{\lambda}X + \frac{\lambda}{2} - \frac{3}{4} + \frac{1}{\sqrt{\lambda}} \quad \text{et} \quad Y + \sqrt{\lambda}X + \frac{\lambda}{2} - \frac{3}{4} - \frac{1}{\sqrt{\lambda}}.$$

que l'on coupe par $Y = X^2$. Cela fournit deux équations du second degré en x :

$$x^2 - \sqrt{\lambda}x + \frac{\lambda}{2} - \frac{3}{4} + \frac{1}{\sqrt{\lambda}} \quad \text{et} \quad x^2 + \sqrt{\lambda}x + \frac{\lambda}{2} - \frac{3}{4} - \frac{1}{\sqrt{\lambda}}.$$

La première admet deux racines imaginaires conjuguées, l'autre deux racines réelles :

$$x = \frac{-\sqrt{\lambda} \pm \sqrt{-\lambda + 3 + 4/\sqrt{\lambda}}}{2},$$

avec $\lambda = 1 + \sqrt[3]{3}$ (valeurs approchées : 0,1014101 et $-1,6641799$).

4.3 Pinceau de coniques et théorème de Pascal

4.3.1 Le théorème de conicité

Une fois encore, nous allons retrouver le théorème de Pascal et faire le lien avec le théorème de Pappus et les relations vues dans la Partie II, ???. On commence par écrire, à l'aide des crochets, l'équation de la conique passant par cinq points en position générale :

4.3.1 Lemme. Soient $a, b, c, d, e \in \mathbf{P}(E)$ des points en position générale (i.e. précisément tels que trois quelconques d'entre eux ne sont pas alignés). Un point m est sur l'unique conique Γ passant par a, b, c, d, e si et seulement s'il vérifie la relation :

$$[a, d, e][b, c, e][a, b, m][c, d, m] - [a, b, e][c, d, e][a, d, m][b, c, m] = 0.$$

Démonstration. Les équations $[a, b, m][c, d, m] = 0$ et $[a, d, m][b, c, m] = 0$ sont respectivement les équations des coniques dégénérées $(ab) \cup (cd)$ et $(ad) \cup (bc)$ du pinceau défini par a, b, c, d . Les coniques du pinceau ont donc pour équations : $\lambda[a, b, m][c, d, m] - \mu[a, d, m][b, c, m] = 0$, avec $\lambda, \mu \in k$ non tous deux nuls. On obtient l'équation de Γ en écrivant qu'elle est dans le pinceau et qu'elle passe par e , ce qui détermine λ et μ à un scalaire près.

4.3.2 Remarque. On peut écrire l'équation ci-dessus sous beaucoup d'autres formes en utilisant la relation à cinq points, cf. 4.2.9.

On déduit du résultat précédent un critère permettant d'affirmer que six points sont sur une conique :

4.3.3 Corollaire. (Critère de conicité⁹) Soient a, b, c, d, e, f six points de $\mathbf{P}(E)$. Ils sont sur une même conique si et seulement si on a la relation :

$$(*) \quad [a, d, e][b, c, e][a, b, f][c, d, f] - [a, b, e][c, d, e][a, d, f][b, c, f] = 0.$$

Démonstration. Lorsque les points sont en position générale, c'est le résultat précédent. Précisément, si trois quelconques des points a, b, c, d, e ne sont pas alignés, il existe une unique conique Γ qui contient ces points et le point f est sur Γ si et seulement si on a la relation $(*)$ en vertu de 4.3.1.

Il reste donc seulement à examiner les cas spéciaux. Notons déjà que si deux des six points sont égaux, il est clair que tous sont sur une conique (c'est 4.1.1) et que la relation $(*)$ est vérifiée (c'est trivial sauf pour $a = c$; $b = d$; $e = f$ où on le vérifie par un calcul immédiat). On supposera désormais que les six points sont distincts.

Supposons que trois parmi les points a, b, c, d, e sont alignés sur une droite D . Notons qu'alors les six points seront sur une conique, soit si l'un des autres points est aussi sur la droite D (le cas 42), soit si les points restant sont alignés (le cas 33). À permutation près, on se ramène aux deux cas suivants.

- Les points a, d, e sont alignés. La relation $(*)$ est vérifiée si et seulement si son deuxième terme est nul. Or, cela signifie, soit que b, c ou f est sur la

⁹Par abus de langage, j'emploierai ce mot pour indiquer que des points sont sur une même conique.

droite ade (cas 42), soit que b, c, f sont alignés (cas 33) et cette nullité est bien équivalente au fait que les six points sont sur une conique.

• Les points a, b, c sont alignés. On peut donc écrire $c = \lambda a + \mu b$, avec λ, μ non nuls puisqu'on a supposé les points distincts. Quitte à changer (les vecteurs) a en λa et b en μb ce qui ne change pas les points et n'altère pas la validité de (*), on peut même supposer $c = a + b$. La relation (*) se traduit alors par :

$$[a, b, e][a, b, f]([a, d, e][b, d, f] - [b, d, e][a, d, f]) = 0.$$

En vertu de la relation à cinq points, voir 4.2.9, le dernier terme s'écrit aussi $[a, b, d][d, e, f]$ et (*) se traduit donc en $[a, b, e][a, b, f][a, b, d][d, e, f] = 0$, ce qui exprime exactement le fait que les six points sont sur une conique (on est dans le cas 42 pour les trois premiers crochets et dans le cas 33 pour le dernier).

4.3.2 Le théorème de Pascal

La clé de la preuve du théorème de Pascal est le résultat suivant, rencontré Partie II à propos du théorème de Pappus (voir ??) :

4.3.4 Proposition. Soient $a, b, c, a', b', c' \in E$. On a la formule :

$$[(b \wedge c') \wedge (b' \wedge c), (c \wedge a') \wedge (c' \wedge a), (a \wedge b') \wedge (a' \wedge b)] = \\ [a, a', b][b, b', c][c, c', a][a', b', c'] - [a, a', c'][b, b', a'][c, c', b'][a, b, c].$$

4.3.5 Corollaire. (Théorème de Pascal)

Si a, b, c, a', b', c' sont six points distincts d'une conique, et si u, v, w sont les points d'intersection des droites (bc') et (cb') , (ca') et (ac') , (ab') et (ba') respectivement, les points u, v, w sont alignés.

Démonstration. On applique ?? en notant que la nullité du premier membre de la relation équivaut à l'alignement de u, v, w et celle du second au fait que les six points sont sur une même conique (on utilise 4.3.3 avec $a = a, b = a', c = b', d = c, e = b$ et $f = c'$).

4.3.3 Remarques sur le critère de conicité

Il y a évidemment un autre polynôme dont la nullité équivaut à la conicité des points a, b, c, d, e, f , c'est le déterminant du système d'équations en les coefficients que ces points définissent. En fait, ce sont les mêmes, au signe près :

4.3.6 Corollaire. Soient $a, b, c, d, e, f \in E$ que l'on écrit sur une base : $a = (a_1, a_2, a_3)$, etc. On pose $a^\# = (a_1^2, a_2^2, a_3^2, a_2a_3, a_3a_1, a_1a_2)$ et de même pour les autres. On a alors l'égalité de polynômes :

$$[a, b, e][c, d, e][a, d, f][b, c, f] - [a, d, e][b, c, e][a, b, f][c, d, f] = \det(a^\#, b^\#, c^\#, d^\#, e^\#, f^\#).$$

Démonstration. On peut supposer le corps k algébriquement clos (quitte à le plonger dans une clôture algébrique \bar{k}). Appelons F le premier polynôme et G le second. Ces polynômes sont nuls, soit si l'un des vecteurs a, \dots, f est nul, soit, sinon, si les 6 points correspondants de $\mathbf{P}(E)$ sont sur une même conique. C'est le résultat précédent en ce qui concerne F , et pour G , c'est le fait que les équations en α, \dots, η du type suivant admettent une solution commune non triviale :

$$\alpha a_1^2 + \beta a_2^2 + \gamma a_3^2 + 2\delta a_2a_3 + 2\epsilon a_3a_1 + 2\eta a_1a_2 = 0.$$

Comme les deux polynômes sont homogènes de degré 2 en chaque paquet de variables a, \dots, f , le Nullstellensatz montre qu'ils sont proportionnels. On conclut qu'ils sont égaux en examinant le terme diagonal de G à savoir $a_1^2b_2^2c_3^2d_2d_3e_3e_1f_1f_2$.

On en déduit aussitôt :

4.3.7 Corollaire. Le polynôme

$$F = [a, d, e][b, c, e][a, b, f][c, d, f] - [a, b, e][c, d, e][a, d, f][b, c, f]$$

est invariant (resp. anti-invariant) par toute permutation paire (resp. impaire) de a, b, \dots, f .

4.3.8 Remarque. Ce résultat d'invariance permet de comprendre un phénomène rencontré Partie II : on peut aussi écrire le second membre de la relation de Pappus ?? sous la forme :

$$[b', c', a][c', a', b][a', b', c][a, b, c] - [b, c, a'][c, a, b'][a, b, c'][a', b', c'].$$

On voit que cette deuxième forme est obtenue à partir de la première en permutant circulairement a, b, c et en laissant fixes a', b', c' .

4.4 Le théorème de Desargues

Nous donnons ici la version définitive du théorème de l'involution de Desargues, en termes de pincesaux de coniques.

4.4.1 Théorème. Soit $\alpha, \beta, \gamma, \delta$ un repère du plan projectif $\mathbf{P}(E)$ et soit D une droite ne passant par aucun des points du repère. On note $a, a'; b, b'; c, c'$ les intersections de D avec les droites $(\alpha\beta), (\gamma\delta); (\alpha\gamma), (\beta\delta); (\alpha\delta), (\beta\gamma)$ respectivement et on suppose $a \neq a'$. Soit Γ une conique passant par $\alpha, \beta, \gamma, \delta$. On suppose que Γ coupe D en des points d, d' (éventuellement confondus). Alors, l'involution f qui échange a et a' et b et b' (et aussi c et c' en vertu de Partie I ??) échange d et d' .

Démonstration. Il suffit de montrer l'égalité des birapports $r := \llbracket a, b, c, d \rrbracket = r' := \llbracket a', b', c', d' \rrbracket$. On a d'abord, par incidence, $r = \llbracket (\alpha a), (\alpha b), (\alpha c), (\alpha d) \rrbracket$, puis, par définition du birapport sur la conique, $r = \llbracket \beta, \gamma, \delta, d \rrbracket$. De l'autre côté on a, pour les mêmes raisons, $r' = \llbracket a', b', c', d' \rrbracket = \llbracket (\gamma a'), (\gamma b'), (\gamma c'), (\gamma d') \rrbracket = \llbracket \delta, u, \beta, d' \rrbracket$ où u est l'autre point d'intersection de Γ et de $(\gamma b')$. La conclusion est alors immédiate en utilisant l'involution $\sigma_{b'}$ de point de Frégier b' qui échange β et δ, γ et u, d et d' .

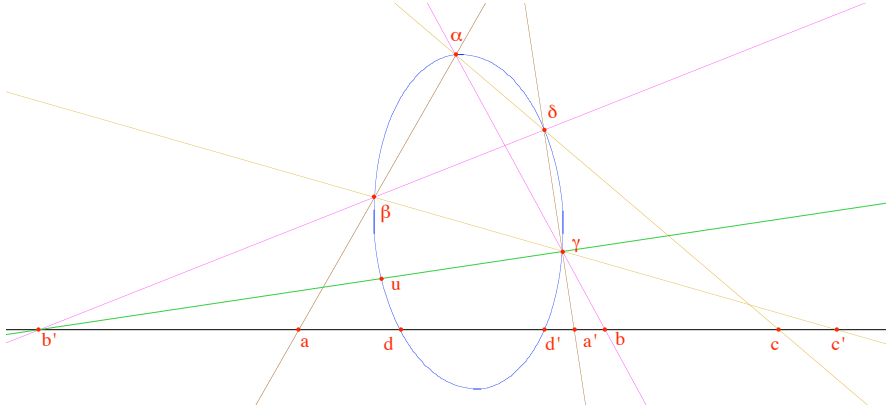


Figure 4.8: Le théorème de Desargues.

On peut reformuler ce théorème sous la forme (classique) suivante :

4.4.2 Corollaire. (théorème de Desargues) Soit $\alpha, \beta, \gamma, \delta$ un repère du plan projectif $\mathbf{P}(E)$ et soit D une droite ne passant par aucun des points du repère. Le pinceau des coniques passant par $\alpha, \beta, \gamma, \delta$ coupe D en des points en involution.

4.5 Le grand théorème de Poncelet

Il s'agit d'un des théorèmes¹⁰ les plus spectaculaires sur les coniques. La preuve donnée ici est dite en termes modernes, mais remonte essentiellement à Jacobi¹¹. Pour avoir une idée de la preuve de Poncelet, voir exercices 4.6.17 et 4.6.18 et [HB87].

4.5.1 La situation et l'énoncé

4.5.1 Notations. On considère deux coniques Ω et C propres et distinctes. Si a est un point de Ω , on parlera des deux tangentes à C issues de a dans les deux cas suivants :

- s'il existe deux tangentes à C distinctes et passant par a ,
- si a est un point commun à Ω et C , les tangentes en question étant alors toutes deux égales à la tangente en a à C .

De plus, si a, b sont deux points de Ω on conserve la convention usuelle s'agissant de la droite (ab) : si a et b sont égaux il s'agit de la tangente en a à Ω .

4.5.2 Définition. Avec les notations précédentes, on appelle **ligne polygonale de Poncelet** (ou simplement *ligne de Poncelet*) inscrite dans Ω et circonscrite à C une suite de points $a_n \in \Omega$ ($n \in \mathbf{Z}$) tels que, pour tout $n \in \mathbf{Z}$, les droites $(a_n a_{n-1})$ et $(a_n a_{n+1})$ soient les deux tangentes à C issues de a_n . Une telle ligne est dite **périodique** de période $s \in \mathbf{N}^*$ si l'on a $a_n = a_{n+s}$ pour tout¹² $n \in \mathbf{Z}$.

Existence de lignes de Poncelet

4.5.3 Proposition. Soit a un point de Ω et supposons qu'il existe une droite D passant par a et tangente à C . Alors, il existe une ligne de Poncelet passant par a .

¹⁰On désigne souvent ce théorème comme le “porisme” de Poncelet. Selon le Littré, la différence entre un théorème et un porisme réside dans le fait qu'un porisme est présenté comme une question ouverte dont il s'agit de trouver la réponse : une graine de théorème en quelque sorte.

¹¹Il semble que Jacobi a mis le doigt un peu par hasard sur le lien entre Poncelet et les fonctions elliptiques : en menant le calcul du théorème de Poncelet dans le cas des cercles et en utilisant les fonctions trigonométriques, il a vu apparaître une formule liée à l'addition des fonctions elliptiques qu'il connaissait bien par ailleurs. Sur l'histoire du théorème de Poncelet, voir [HB87].

¹²Une récurrence immédiate montre qu'il suffit qu'on ait cette propriété pour un n .

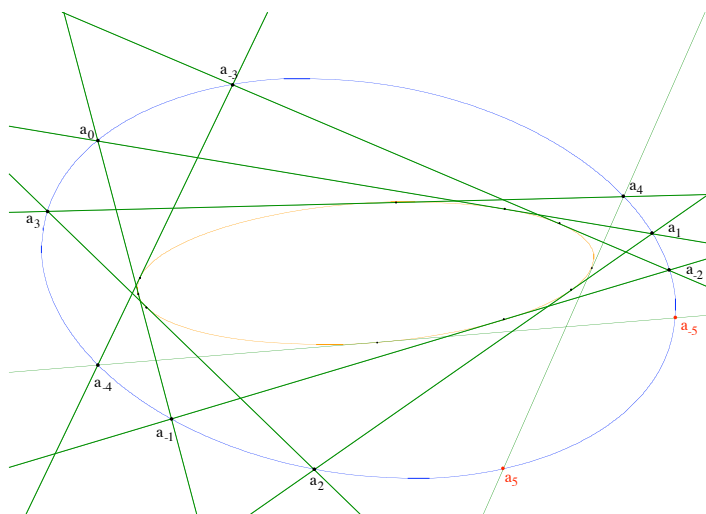


Figure 4.9: Une ligne polygonale de Poncelet

Démonstration. On pose $a_0 = a$. Il y a une ou deux tangentes à C issues de a . On appelle a_1 l'autre¹³ point d'intersection de D et de Ω et a_{-1} l'autre point d'intersection de l'autre tangente à C issue de a (là encore la tangente peut être égale à D et a_{-1} peut être égal à a_0). En recommençant cette opération à partir de a_1 et a_{-1} on montre par récurrence l'existence de la ligne polygonale.

Le théorème de Poncelet

4.5.4 Théorème. *Avec les notations précédentes, s'il existe une ligne de Poncelet périodique de période s , toutes les lignes de Poncelet sont périodiques¹⁴ de période s .*

4.5.2 Le cadre de la preuve

¹³Si les coniques sont tangentes en a , on a $a_1 = a_0$ et la ligne est réduite à sa plus simple expression.

¹⁴Voici la version originale du théorème (page 249 du Traité des propriétés projectives, cinquième cahier) : *Il est impossible, généralement parlant, d'inscrire à une courbe donnée du deuxième degré un polygone qui soit en même temps circonscrit à une courbe de ce degré, et quand la disposition particulière de ces courbes sera telle que l'inscription et la circonscription simultanée soient possibles pour un seul polygone essayé à volonté, il y en aura, par là même, une infinité jouissant de cette propriété à l'égard des coniques données.*

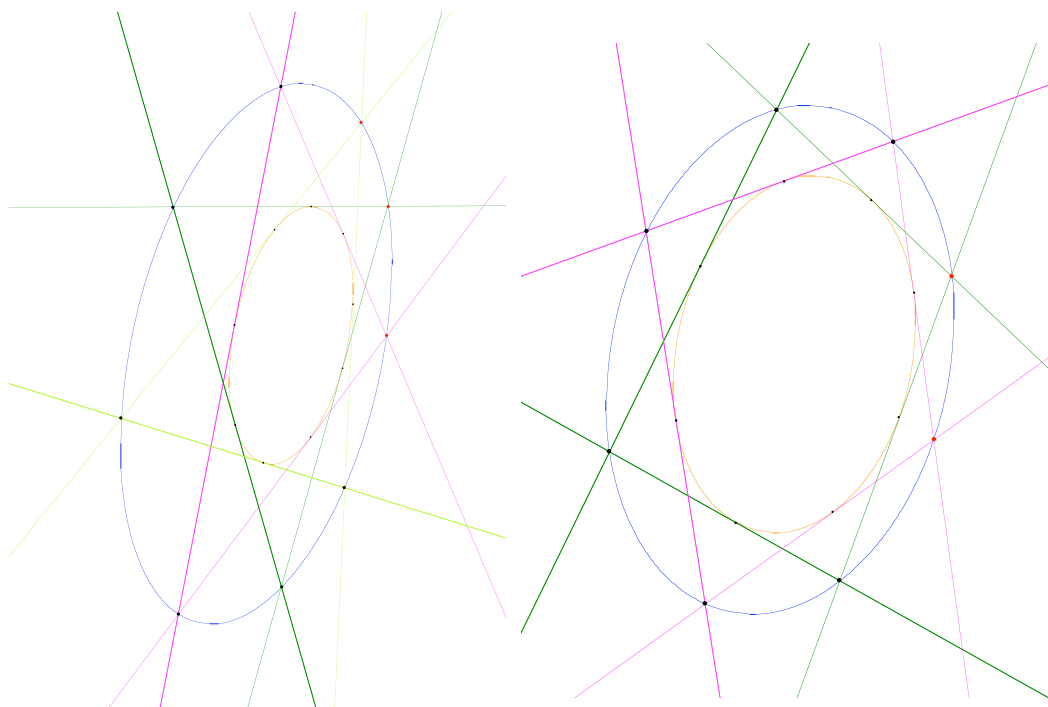


Figure 4.10: Lignes de Poncelet de périodes 3 et 4

Réduction au cas algébriquement clos

On peut plonger k dans un corps algébriquement clos \bar{k} (théorème de Steinitz, voir Partie II ??). On en déduit (par exemple en choisissant un repère) un plongement de l'espace $E \simeq k^3$ dans $\bar{E} \simeq \bar{k}^3$ et de $\mathbf{P}(E)$ dans $\mathbf{P}(\bar{E})$. On note $\bar{\Omega}$ et \bar{C} les coniques obtenues en étendant ainsi les scalaires à \bar{k} . Supposons le théorème de Poncelet établi sur \bar{k} et soit (a_n) une ligne de Poncelet dont les points sont à coefficients dans k . Si cette ligne est périodique, il en est de même de toutes les lignes de Poncelet à coefficients dans \bar{k} , donc *a fortiori* de celles qui sont à coefficients dans k .

On supposera désormais que le corps k est algébriquement clos.

Une hypothèse supplémentaire

Nous ferons l'hypothèse simplificatrice que les coniques Ω et C sont **transverses** (autrement dit qu'elles se coupent en quatre points distincts).

Le théorème reste vrai sans cette hypothèse, voir [Ber90] §16.6 ou ci-dessous exercices 4.6.13, 4.6.14, 4.6.15, 4.6.16.

Le principe de la preuve, 1 : la variété d'incidence V et l'application de Poncelet F

Rappelons qu'on note C^* la conique duale de C . Il s'agit de la conique de $\mathbf{P}(E^*)$ dont les points sont les droites tangentes à C .

4.5.5 Définition. On appelle **variété d'incidence** et on note $V(\Omega, C^*)$ ou simplement V , l'ensemble des couples $(m, D) \in \Omega \times C^*$ (c'est-à-dire un point de Ω et une tangente à C) qui vérifient $m \in D$.

La variété d'incidence permet de surmonter le double dilemme auquel on est aussitôt confronté dès qu'on travaille sur la question : tracer une ligne de Poncelet en partant d'un point de Ω ou d'une tangente à C , certes, mais de quel côté partir ?

La proposition évidente suivante permet de définir l'application de Poncelet :

4.5.6 Proposition-Définition. Soient V la variété d'incidence, (m, D) un point de V , m' le point de Ω (éventuellement confondu avec m) où D recoupe Ω et D' la deuxième tangente à C issue de m' (éventuellement confondue avec D).

L'application $F_1 : V \rightarrow V$ (resp. $F_2 : V \rightarrow V$) qui à (m, D) associe (m', D) (resp. à (m', D) associe (m', D')) est une involution de V .

L'application $F : V \rightarrow V$ définie par la formule $F = F_2 \circ F_1$, ou encore $F(m, D) = (m', D')$ est dite **application de Poncelet** de V .

Cette application formalise la construction des lignes polygonales de Poncelet :

4.5.7 Proposition. Soit (a_n) une ligne polygonale de Poncelet inscrite dans Ω et circonscrite à C .

On a, pour tout $n \in \mathbf{Z}$: $F(a_n, (a_n a_{n+1})) = (a_{n+1}, (a_{n+1} a_{n+2}))$. On en déduit, pour tout $s \geq 0$ et tout $n \in \mathbf{Z}$, $F^s(a_n, (a_n a_{n+1})) = (a_{n+s}, (a_{n+s} a_{n+s+1}))$. En particulier, on a, pour tout $s \geq 0$, $(a_s, (a_s a_{s+1})) = F^s(a_0, (a_0 a_1))$.

L'introduction de la variété d'incidence et de l'application de Poncelet va permettre de reformuler très simplement le théorème de Poncelet :

4.5.8 Théorème. S'il existe un élément $(m, D) \in V$ et un entier $s \geq 1$ tels que $F^s(m, D) = (m, D)$ on a $F^s = \text{Id}_V$.

Le principe de la preuve, 2 : la structure de groupe sur V

Le ressort de la preuve est la proposition suivante :

4.5.9 Proposition. *La variété d'incidence V est munie d'une structure de groupe abélien dont la loi est notée \oplus et il existe $B \in V$ tel que l'application F soit donnée par la formule $F(P) = P \oplus B$.*

Le théorème de Poncelet est conséquence évidente de cette proposition. En effet, une récurrence immédiate montre qu'on a $F^s(P) = P \oplus sB$ pour tout $P \in V$ et tout $s \in \mathbf{N}$. Dire qu'on a, pour un $P_0 \in V$ particulier, $F^s(P_0) = P_0$ signifie donc qu'on a $sB = O$, où O désigne l'élément neutre de V , ou encore que B est un élément d'ordre s de V et il en résulte qu'on a $F^s(P) = P$ pour tout P , donc $F^s = \text{Id}_V$.

4.5.3 Preuve du théorème de Poncelet : les personnages

La preuve du théorème que nous donnons ci-dessous consiste à expliciter la variété d'incidence V et à ramener sa structure de groupe à celle d'une cubique plane vue en 3.5.27. En vérité, cette preuve est sous-tendue par des considérations de géométrie algébrique un peu plus avancées que nous indiquerons au fil de la preuve. Rappelons qu'on a supposé que le corps est algébriquement clos et que les coniques sont transverses.

4.5.10 Notations. Nous adopterons les notations suivantes. Dans le plan projectif de départ où habitent les coniques Ω et C , les coordonnées seront notées x, y, t avec des minuscules. Dans le plan dual, les coordonnées seront u, v, w . Nous passerons ensuite dans l'espace projectif \mathbf{P}^3 où nous utiliserons les coordonnées X, Y, Z, T , puis nous projeterons l'espace sur un plan projectif avec les coordonnées X, Y, Z .

Des équations pour les coniques

4.5.11 Proposition. *Dans un repère convenable, les coniques Ω et C ont respectivement pour équations $y^2 - xt = 0$ et $\alpha y^2 + 2\beta yt + \gamma t^2 - 2xy = 0$ avec $\gamma \neq 0$. La conique duale C^* a pour équation $(\alpha\gamma - \beta^2)u^2 + 2\gamma uv - 2\beta uw - w^2 = 0$.*

Démonstration. On choisit un point d'intersection a de Ω et C . On note c le second point d'intersection de Ω et de la tangente en a à C (cette droite n'est pas tangente à Ω par transversalité). Soit b le point d'intersection des

tangentes à Ω en a et c et d un point¹⁵ de Ω distinct de a, c . On choisit a, b, c, d comme repère. Alors, la conique Ω a pour équation $y^2 - xt = 0$ (on est dans la situation de 2.2.24). La conique C passant par a et tangente à (ac) n'a pas de terme en x^2 ni en xt . En revanche, ses termes en xy et t^2 sont non nuls (sinon elle serait dégénérée). Quitte à multiplier par un scalaire on peut supposer que le terme en xy est $-2xy$ et on a l'équation annoncée.

On en déduit l'équation, en u, v, w , de la conique duale C^* en calculant la matrice inverse de celle de la forme quadratique qui définit C , voir 2.2.21.

Paramétrer les coniques

La conique Ω a un paramétrage évident : $x = \lambda^2$, $y = \lambda\mu$, $t = \mu^2$. Pour C^* , on note qu'elle passe par le point $(u, v, w) = (0, 1, 0)$ et on coupe C^* par une droite variable passant par ce point : $\eta u - \xi w = 0$. On obtient le paramétrage en (ξ, η) suivant :

$$u = 2\gamma\xi^2, \quad v = \eta^2 + 2\beta\xi\eta + (\beta^2 - \alpha\gamma)\xi^2, \quad w = 2\gamma\xi\eta.$$

Projection, points-bases et coniques dégénérées

On considère la variété d'incidence V et sa projection $p : V \rightarrow \Omega$ qui à (m, D) associe m . En général, les fibres $p^{-1}(m)$ contiennent deux éléments (m, D) et (m, D') où D et D' sont les deux tangentes à C issues de m (on dit que p est un **revêtement de degré 2**), sauf lorsque m est l'un des quatre points d'intersection de Ω et C (les points-base du pinceau défini par Ω et C), auquel cas il n'y a qu'un point (m, D) , D étant la tangente à C en m (on dit que p est **ramifié en les points de $\Omega \cap C$**). Ces points sont déterminés ainsi :

4.5.12 Proposition. *1) Les points d'intersection de Ω et C sont le point $a = (1, 0, 0)$ de paramètre $(1, 0)$ et les points de Ω de paramètre $(\lambda, 1)$ avec λ solution de l'équation :*

$$P(\lambda) = 2\lambda^3 - \alpha\lambda^2 - 2\beta\lambda - \gamma = 0.$$

¹⁵On peut choisir pour d un point d'intersection de Ω et C distinct de a . Cela impose entre les paramètres α, β, γ la relation $\alpha + 2\beta + \gamma = 2$, qui traduit que C passe par d . On retrouve le fait que la situation dépend de deux paramètres, voir 4.2.13. Dans la pratique, les calculs ne sont pas plus simples avec cette condition supplémentaire.

Les coniques sont transverses¹⁶ si et seulement si ces points sont distincts, c'est-à-dire si le discriminant Δ de P est non nul, avec :

$$\Delta = 4\alpha^2\beta^2 + 64\beta^3 - 4\alpha^3\gamma - 108\gamma^2 - 72\alpha\beta\gamma.$$

2) Soit $m \in \Omega$ un point distinct de a , de paramètre $(\lambda, 1)$. La droite (am) est la droite d'équation $y - \lambda t = 0$. Cette droite est tangente en a à une unique conique C_m du pinceau défini par Ω et C et cette conique a pour matrice $C - 2\lambda\Omega$ (en notant encore Ω et C les matrices des formes quadratiques définissant ces coniques).

3) La conique C_m est dégénérée si et seulement si m est l'un des points-base du pinceau autres que a , c'est-à-dire si l'on a $\det(C - 2\lambda\Omega) = P(\lambda) = 0$.

Démonstration. Le point 1) s'obtient en remplaçant (x, y, t) par $(\lambda^2, \lambda\mu, \mu^2)$ dans l'équation de C . Si l'on écarte la solution $\mu = 0$ qui correspond à a , on peut supposer $\mu = 1$ et les autres points correspondent aux solutions de $P(\lambda) = 0$. Le calcul du discriminant est facile (voir par exemple [Lan69]).

2) Il est clair que (am) a pour équation $y - \lambda t = 0$. Pour montrer que c'est la tangente en a à la conique $C - 2\lambda\Omega$ on écrit l'équation affine de cette conique dans le plan $x = 1$:

$$(\alpha - 2\lambda)y^2 + 2\beta yt + \gamma t^2 - 2(y - \lambda t) = 0$$

et on voit que la tangente au point $(0, 0)$ est bien donnée par $y - \lambda t$.

Le point 3) est clair car les coniques dégénérées du pinceau sont les paires de droites joignant les points bases et leurs tangentes en a sont les droites qui joignent a aux autres points d'intersection de Ω et C . On a donc l'équivalence $P(\lambda) = 0 \iff \det(C - 2\lambda\Omega) = 0$ et on vérifie en calculant le déterminant que ces polynômes sont égaux.

Plonger le produit $\Omega \times C^*$ dans \mathbf{P}^3

Les paramétrages précédents réalisent des isomorphismes de Ω et C^* sur \mathbf{P}^1 . On peut alors plonger $\Omega \times C^* \simeq \mathbf{P}^1 \times \mathbf{P}^1$ dans \mathbf{P}^3 par le plongement de Segre déjà utilisé dans la Partie II :

$$(\lambda, \mu; \xi, \eta) \mapsto (\lambda\xi, \lambda\eta, \mu\xi, \mu\eta).$$

Si l'on note X, Y, Z, T les variables dans \mathbf{P}^3 , l'image du produit est la quadrique d'équation $(*) : \psi(X, Y, Z, T) := XT - YZ = 0$.

¹⁶Rappelons que nous supposons cette hypothèse réalisée.

Plonger la variété d'incidence

Le plongement précédent permet de plonger aussi la variété d'incidence V dans \mathbf{P}^3 . Il y a une équation supplémentaire $ux + vy + wt = 0$ qui exprime que le point est sur la tangente. Cette équation a une traduction avec les paramètres :

$$2\gamma\lambda^2\xi^2 + \lambda\mu\eta^2 + 2\beta\lambda\mu\xi\eta + (\beta^2 - \alpha\gamma)\lambda\mu\xi^2 + 2\gamma\mu^2\xi\eta = 0$$

qui donne en X, Y, Z, T l'équation :

$$(**) \quad \varphi(X, Y, Z, T) = YT + 2\beta XT + (\beta^2 - \alpha\gamma)XZ + 2\gamma X^2 + 2\gamma ZT = 0.$$

La variété V est donc isomorphe à la courbe intersection des deux quadriques définies par ψ et φ . Cette courbe sera notée W et on a un isomorphisme $\sigma : V \rightarrow W$. Il s'agit d'une courbe de degré 4 de \mathbf{P}^3 . Cela signifie que si on coupe W par un plan on trouve quatre points d'intersection (comptés avec leurs multiplicités). En effet, dans le plan de coupe, on est ramené à l'intersection de deux coniques.

Les tangentes à W sont les intersections des plans tangents aux surfaces d'équations ψ et φ et elles sont données par les dérivées partielles de ψ i.e. $(T, -Z, -Y, X)$ et de φ , i.e. $(2\beta T + (\beta^2 - \alpha\gamma)Z + 4\gamma X, T, (\beta^2 - \alpha\gamma)X + 2\gamma T, Y + 2\beta X + 2\gamma Z)$.

On note que la courbe W contient trois points du repère de \mathbf{P}_k^3 : $O = (0, 1, 0, 0)$, $B = (0, 0, 1, 0)$ et $A = (0, 0, 0, 1)$.

Projection sur le plan

On considère la projection $\pi_0 : \mathbf{P}^3 - \{A\} \rightarrow \mathbf{P}^2$ qui associe à un point P distinct de A le point d'intersection de la droite (AP) avec le plan $T = 0$. Cette application est définie par $\pi_0(X, Y, Z, T) = (X, Y, Z)$. On désigne par π sa restriction à W . Pour calculer l'image Γ_0 de W par π on élimine la variable T en la remplaçant par $\frac{YZ}{X}$ dans l'équation $(**)$ et on multiplie par X pour chasser les dénominateurs. On obtient la courbe d'équation :

$$Y^2Z + 2\beta XYZ + (\beta^2 - \alpha\gamma)X^2Z + 2\gamma X^3 + 2\gamma YZ^2 = 0.$$

Il s'agit d'une cubique plane. On notera que le morphisme π n'est pas défini en A mais qu'on peut le prolonger en ce point en remplaçant la droite (AP) par la tangente à W en A . Cette tangente a pour équations $X = Y + 2\gamma Z = 0$ et l'image de A est donc le point $(0, -2\gamma, 1)$.

4.5.13 Proposition. *L'application $\pi : W \rightarrow \Gamma_0$ est bijective.*

Démonstration. L'application réciproque de π est évidente sur l'ouvert $X \neq 0$ de Γ_0 . En effet, on associe à $(X, Y, Z) \in \Gamma_0$ le point $(X, Y, Z, \frac{YZ}{X})$ de W . Pour les points de la droite $X = 0$ l'application réciproque est donnée par $(0, 0, 1) \mapsto (0, 0, 1, 0) = B$, $(0, 1, 0) \mapsto (0, 1, 0, 0) = O$ et $(0, -2\gamma, 1) \mapsto A$.

4.5.14 Remarque. En vérité, l'application π est un isomorphisme de W sur Γ_0 . Comme ce sont des courbes projectives lisses, cela résulte de [Har77] I 6.8. Pour une preuve directe, voir l'exercice 4.6.10.

Le changement de variable $Y' = Y + \beta X + \gamma Z$ transforme Γ_0 en la courbe Γ d'équation :

$$Y'^2 Z + \gamma(2X^3 - \alpha X^2 Z - 2\beta X Z^2 - \gamma Z^3) = 0,$$

soit $Y'^2 Z + \gamma \hat{P}(X, Z) = 0$ où \hat{P} est l'homogénéisé du polynôme de degré 3 rencontré en 4.5.12. Comme on a supposé les coniques transverses, ce polynôme admet trois racines distinctes (voir 4.5.12) de sorte que la cubique Γ est non singulière. On reconnaît une courbe elliptique comme celle vue en 3.5.27.

4.5.15 Remarques. 1) La réapparition du polynôme P n'est pas fortuite. En effet, on a vu que les zéros de ce polynôme sont les points de ramification de la projection p de V dans Ω qui, en identifiant V à $\mathbf{P}^1 \times \mathbf{P}^1$ et Ω à \mathbf{P}^1 par les paramétrages, associe (λ, μ) à $(\lambda, \mu), (\xi, \eta)$. On peut transporter p en utilisant les isomorphismes $V \simeq W \simeq \Gamma_0 \simeq \Gamma$. Sur W , cette projection est donnée par $p_1(X, Y, Z, T) = (X, Z) = (\xi\lambda, \xi\mu) = (Y, T) = (\eta\lambda, \eta\mu) = (\lambda, \mu)$ (comme l'un des deux nombres ξ, η est non nul, p_1 est bien défini sur W). Sur Γ_0 et Γ , on obtient la projection p_2 qui à (X, Y, Z) associe (X, Z) , sauf pour $\omega = (0, 1, 0)$ qui s'envoie sur $(1, 0)$. Cette projection est ramifiée en quatre points : le point "à l'infini" ω et les trois points $(X, 0, Z)$ qui vérifient $P(X, Z) = 0$ (pour ces points, il y a un unique Y tel que (X, Y, Z) soit sur $\Gamma : Y = 0$).

2) Quand on est plus savant, on peut retrouver le fait que V est une courbe de genre 1 (donc elliptique) grâce à cette projection et à la formule d'Hurwitz (voir [Har77]). Comme la projection $p : V \rightarrow \Omega$ est un revêtement de degré deux, ramifié quatre points, cette formule donne : $2g_V - 2 = 2(2g_\Omega - 2) + 4 = 0$ et on trouve bien $g_V = 1$.

La loi de groupe sur W

On a vu en 3.5.27 que, si l'on se donne un point de la cubique Γ , on a une loi de groupe sur Γ dont ce point est l'élément neutre. On utilisera ici

$\omega = (0, 1, 0)$. La bijection $\pi : W \rightarrow \Gamma$ permet de transporter cette loi sur W avec comme élément neutre $O = (0, 1, 0, 0)$. Précisément, la définition est la suivante : soient $P, Q \in W$. On considère le plan¹⁷ (P, Q, A) . Il recoupe la courbe W en un quatrième point R . On considère alors le plan (R, A, O) . Il recoupe W en le point $P \oplus Q$.

4.5.16 Proposition. *La loi \oplus fait de W un groupe abélien dont l'élément neutre est O .*

Démonstration. Cela résulte, par contre-projection, c'est-à-dire par application de π^{-1} , de l'assertion analogue sur Γ .

4.5.4 Preuve du théorème de Poncelet : le calcul de l'application de Poncelet

Il s'agit maintenant de calculer l'application F . Le lecteur pressé pourra sauter directement au paragraphe où ce calcul est mené, mais s'il souhaite en comprendre vraiment le ressort, il peut aussi lire les deux paragraphes suivants. Il est cependant averti qu'ils font appel à des notions de géométrie algébrique un peu plus avancées, qu'il pourra admettre sans encombre.

La loi de groupe, version savante

Une autre façon de concevoir la loi de groupe sur une courbe elliptique Γ est de parler de diviseurs. Nous avons rencontré cette notion dans le cas particulier de l'intersection de deux coniques, voir 4.1.17. Pour le cas général, le lecteur consultera [Ful69] ou [Har77] ou [Per95]. On appelle $\text{Div}(\Gamma)$ le groupe des diviseurs de Γ . Ses éléments sont les combinaisons linéaires formelles finies $\sum_{P \in \Gamma} n_P P$ où les n_P sont dans \mathbf{Z} et presque tous nuls. Le degré d'un diviseur est l'entier $\sum n_P$. Parmi ces diviseurs il y a les diviseurs (dits principaux) des fonctions rationnelles sur Γ . Pour une telle fonction f , $\text{div}(f)$ est la somme formelle des zéros de f (affectés de leurs multiplicités et munis du signe $+$) et des pôles (affectés du signe $-$). Ces diviseurs sont de degré 0. Le quotient du groupe des diviseurs de degré 0 par les diviseurs principaux est le groupe de Picard (ou jacobienne) de Γ , et on le note $\text{Pic}(\Gamma)$. Nous aurons besoin de préciser ces objets dans deux cas : celui d'une courbe rationnelle et celui d'une courbe elliptique.

Dans le cas rationnel, le groupe de Picard est nul :

¹⁷Si deux des points P, Q, A sont égaux, on les remplace par la tangente en ce point. Si on a $P = Q = A$, on utilise le plan osculateur à W en A , c'est-à-dire le plan $Y + 2\beta X + 2\gamma Z = 0$.

4.5.17 Proposition. Soit Γ une courbe rationnelle (i.e. isomorphe à \mathbf{P}^1 , par exemple une conique). Le groupe $\text{Pic}(\Gamma)$ est nul. En particulier, si P et Q sont deux points de Γ , il existe une fonction rationnelle nulle en P et admettant un pôle en Q .

Inversement, si Γ est une courbe lisse et s'il existe $P, Q \in \Gamma$, distincts, avec $P \sim Q$ dans $\text{Pic}(\Gamma)$, la courbe est rationnelle.

Démonstration. Le sens direct est facile. On peut prendre $\Gamma = \mathbf{P}^1$ et supposer $P = (a, 1)$ et $Q = (b, 1)$. La fraction rationnelle $\frac{x-a}{x-b}$ convient. Pour la réciproque, voir les références citées ci-dessus.

Dans le cas d'une courbe elliptique le groupe de Picard est naturellement en bijection avec la courbe :

4.5.18 Proposition. Soit Γ une courbe elliptique et soit $O \in \Gamma$. L'application $\Phi : P \mapsto P - O$ est une bijection de Γ sur $\text{Pic}(\Gamma)$.

Démonstration. L'application Φ est injective. Sinon, on a P, Q distincts tels que $P - O \sim Q - O$ soit $P \sim Q$. Mais cela implique que la courbe est rationnelle en vertu de 4.5.17.

L'application Φ est surjective. Si $D = P_1 + \dots + P_r - Q_1 - \dots - Q_r$ est un diviseur de degré 0, il s'agit de montrer qu'il est équivalent à un diviseur de la forme $P - O$. On considère le diviseur $D + O$. Il est de degré 1 et le théorème de Riemann-Roch (voir *loc. cit.*) montre qu'il existe une fonction rationnelle f telle que f n'ait de pôles qu'en les P_i et O et s'annule en les Q_i . Elle s'annule donc en un autre point P , qui convient.

4.5.19 Remarque. La bijection précédente permet de transporter la loi de groupe de $\text{Pic} \Gamma$ en une loi de groupe \oplus sur Γ dont l'élément neutre est O . Si P, Q sont dans Γ , le diviseur $P + Q$ est équivalent à $O + R$ (car $P + Q - 2O$ est équivalent à $R - O$, c'est le point non trivial) et on pose $R = P \oplus Q$. Dans le cas d'une cubique plane, cette loi de groupe est identique à celle qui a été définie en 3.5.27. En effet, considérons deux points P, Q de Γ et la droite (PQ) d'équation g . Elle recoupe Γ en $P \vee Q$. On considère la droite $(O(P \vee Q))$ d'équation h . Elle recoupe Γ en R et R est la somme de P et Q au sens de 3.5.27. Si f est la fonction rationnelle $f = g/h$, on a $\text{div} f = P + Q + (P \vee Q) - (O + (P \vee Q) + R)$. Comme ce diviseur est équivalent à 0 on a $P + Q \sim O + R$, de sorte que R est aussi la somme de P et Q au sens défini à l'aide des diviseurs.

La formule pour F , version savante

Le calcul de F , à condition d'interpréter le groupe comme le groupe de Picard, est très facile dans le cas de la variété d'incidence V . Rappelons que V (qui est une courbe elliptique) est contenue dans $\Omega \times C^*$ et donc munie de deux projections $p : V \rightarrow \Omega$ et $q : V \rightarrow C^*$.

4.5.20 Proposition. *Soit $O \in V$. On munit V de la loi de groupe au sens de 4.5.19 pour laquelle O est élément neutre et on pose $B = F(O)$. On a la formule $F(P) = P \oplus B$.*

Démonstration. On commence par un lemme :

4.5.21 Lemme. *Soient $a, a' \in \Omega$ (resp. $D, D' \in C^*$). Alors, les diviseurs $p^{-1}(a)$ et $p^{-1}(a')$ (resp. $q^{-1}(D)$ et $q^{-1}(D')$) sont égaux dans $\text{Pic}(V)$.*

Démonstration. Comme Ω et C^* sont rationnelles, on a $a \sim a'$ et $D \sim D'$, ce qui signifie qu'il existe des fonctions rationnelles f sur Ω et g sur C^* admettant respectivement a et D comme zéros et a' et D' comme pôles. Mais alors, les fonctions rationnelles $f \circ p$ et $g \circ q$ admettent comme diviseurs $p^{-1}(a) - p^{-1}(a')$ et $q^{-1}(D) - q^{-1}(D')$, de sorte que ces diviseurs sont équivalents à 0.

Reprenons la preuve de la proposition. On se reportera à la figure ci-dessous. Notons tout d'abord, avec les notations de 4.5.6, que deux points distincts $P, P' \in V$ ont même image par q si et seulement si ils sont échangés par l'involution F_1 : ce sont deux couples $P = (a, D)$ et $P' = (a', D)$ avec la même tangente. De même, $P', P'' \in V$ ont même image par p s'ils sont échangés par F_2 , car cette fois ils ont en commun le même point : $P' = (a', D)$, $P'' = (a', D')$. On a alors $P' = F_1(P)$, $P'' = F_2(P') = F(P)$.

On pose $O = (a_0, D_0)$. Le point a_0 est sur Ω et la droite D_0 est l'une des tangentes à C par a_0 , voir figure ci-dessous. La droite D_0 recoupe Ω en a_1 et on appelle D_1 l'autre tangente à C issue de a_1 . On a $F_1(O) = (a_1, D_0) := A$, $F_2(A) = (a_1, D_1) := B$, donc $F(O) = B$. On a donc $q^{-1}(D_0) = \{O, A\}$, ou encore, en termes de diviseurs, $q^{-1}(D_0) = O + A$. De même, on a $p^{-1}(a_1) = A + B$.

De même, on a $q^{-1}(D) = P + P'$ et $p^{-1}(a') = P' + P''$. En vertu du lemme on a donc les diviseurs équivalents : $O + A \sim P + P'$ et $A + B \sim P' + P''$. Par différence, on obtient $P - O \sim P'' - B$, soit $P + B = P'' + O$, autrement dit, dans V , $P'' = F(P) = P \oplus B$ comme annoncé.

4.5.22 Remarques.

1) Si l'on a choisi pour a_0 l'un des points d'intersection des coniques Ω et C , on vérifie qu'on a $B = -A$. En effet, il s'agit de montrer la formule $F(A) = O$.

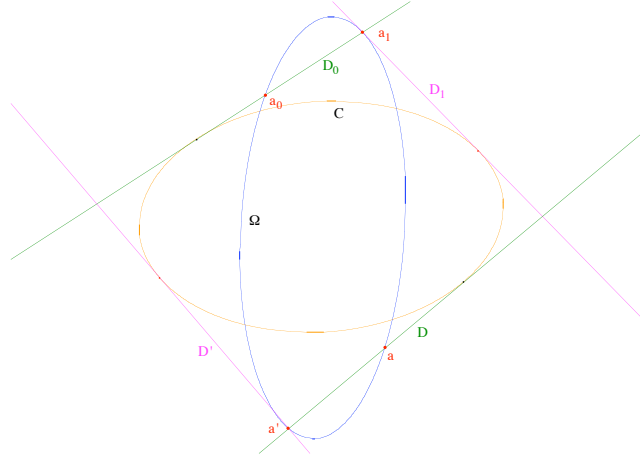


Figure 4.11: Calcul de l'application de Poncelet

Or, on a $F_1(A) = (a_0, D_0) = O$ et $F_2(O) = O$ (comme a_0 est sur C , il n'y a qu'une tangente à C issue de a_0).

2) Une autre preuve du résultat consiste à montrer que les involutions¹⁸ F_i sont nécessairement de la forme $P \mapsto M_i - P$. Cela résulte par exemple de [Har77] IV 4.9 et IV 4.18. On a alors $M_1 = A$ puis $M_2 = A + B$, donc $F(P) = (A + B - (A - P)) = B + P$.

La formule pour F , version calculatoire

On travaille sur W . Rappelons qu'on a $O = (0, 1, 0, 0)$, $A = (0, 0, 0, 1)$ et $B = (0, 0, 1, 0)$. Le théorème suivant a pour conséquence la proposition 4.5.9, donc aussi le théorème de Poncelet 4.5.4 ou 4.5.8 :

4.5.23 Théorème. *On a $F(O) = B$ et, pour tout $P \in W$, les formules $F(P) = P \oplus B$ et $F^n(P) = P \oplus nB$.*

Démonstration. La preuve copie celle de 4.5.20. On utilise les notations de 4.5.6 et on a le lemme suivant :

4.5.24 Lemme. *Soit $P \in W$.*

- 1) *On pose $P' = F_1(P)$. On a la formule $P \oplus P' = A$.*
- 2) *On pose $P'' = F_2(P') = F(P)$. On a la formule $P' \oplus P'' = A \oplus B = O$.*

Le théorème résulte aussitôt de ce lemme. En effet, on a $F(P) = F_2 \circ F_1(P) = P'' = -P' = -(A - P) = P - A = P \oplus B$.

¹⁸C'est vrai pour toutes les involutions d'une courbe elliptique.

Démonstration. (du lemme)

1) Le point P est image de $(a, D) \in V$. Avec les représentations paramétriques de Ω et C^* on a $a = (\lambda, \mu)$ et $D = (\xi, \eta)$, donc $P = (\lambda\xi, \lambda\eta, \mu\xi, \mu\eta)$. Si $P' = F_1(P)$, on a $P' = (a', D)$ où a' est le point où D recoupe Ω . Si les paramètres¹⁹ de a' sont λ', μ' on a $P' = (\lambda'\xi, \lambda'\eta, \mu'\xi, \mu'\eta)$. Pour calculer $P \oplus P'$, on considère le plan (P, P', A) , dont on voit aussitôt qu'il a pour équation $\eta X - \xi Y = 0$. Ce plan recoupe W en un quatrième point, qui n'est autre que B . On considère alors le plan (O, A, B) d'équation $X = 0$ et on cherche ses intersections avec W . Les équations sont $X = YZ = T(Y + 2\gamma Z) = 0$, les points d'intersections sont O, A, B , mais un calcul local dans l'ouvert affine $t = 1$ donne $y = -2\gamma z$ et les équations $x = -2\gamma z^2 = 0$, ce qui montre que le point A est double dans l'intersection²⁰. C'est donc lui le quatrième point cherché, d'où $P \oplus P' = A$.

2) Calculons d'abord $A \oplus B$. On considère le plan (A, A, B) tangent en A à W et passant par B . C'est le plan $X = 0$. Il recoupe W en O . On calcule ensuite le plan (O, O, A) tangent en O à W et passant par A , c'est le plan $Z = 0$.

L'intersection est donnée par les équations $Z = XT = YT + 2\gamma X^2 = 0$. On trouve le point A et le point O . Ce dernier est triple comme on le voit en calculant dans l'ouvert affine $y = 1$ où l'on a $t = -2\gamma x^2$ et les équations $z = -2\gamma x^3 = 0$. On en déduit²¹ $A \oplus B = O$.

Le point P' est image de (a', D) , de paramètres (λ', μ') , (ξ, η) . On a donc $P' = (\lambda'\xi, \lambda'\eta, \mu'\xi, \mu'\eta)$. Dire que $P'' = F_2(P')$ signifie qu'on a $P'' = (a', D')$ où D' est la deuxième tangente à C passant par a' . Le point P'' est donc de la forme $P'' = (\lambda'\xi', \lambda'\eta', \mu'\xi', \mu'\eta')$ (voir exercice 4.6.11 pour un calcul explicite de ξ', η'). On voit que le plan (A, P', P'') a pour équation $\mu'X - \lambda'Z = 0$ et qu'il recoupe W en O . Le même calcul que ci-dessus montre qu'on a $P' \oplus P'' = O$.

Existence de lignes de période 2, 3 ou 4

La formule $F^n(P) = P \oplus nB$ montre qu'il existe des lignes de période s si et seulement si on a $sB = O$ dans l'une quelconque des variantes du groupe $(V, W, \Gamma_0$ ou $\Gamma)$.

On voit déjà qu'il n'existe pas de ligne de période 2. En effet, il faudrait pour cela avoir $2B = O$, soit $B = -B$. Or, on a vu ci-dessus qu'on a $A \oplus B = O$, soit $A = -B$, et on conclut en notant que A et B sont distincts.

¹⁹Il est inutile de les calculer, mais c'est facile, voir exercice 4.6.11.

²⁰Où simplement : A est obtenu à la fois avec $Y = 0$ et avec $Z = 0$.

²¹Une autre voie consiste à utiliser la projection sur la cubique Γ . Les images de A et B étant respectivement $(0, -\gamma, 1)$ et $(0, \gamma, 1)$, elles sont opposées dans le groupe, cf. 3.5.27.

Pour les périodes 3 et 4, on a la proposition suivante :

4.5.25 Proposition. *Avec les notations précédentes, les lignes de Poncelet associées à Ω et C sont de période 3 (resp. 4) si et seulement si on a $\alpha\gamma - \beta^2 = 0$ (resp. $\alpha\beta\gamma - \beta^3 + 2\gamma^2 = 0$).*

Démonstration. Il s'agit essentiellement de calculer $B \oplus B$. On peut faire le calcul dans Γ ou dans W . Faisons le par exemple dans Γ (voir exercice 4.6.12 pour le calcul dans W).

On note encore O, A, B les images de ces points dans Γ . On a $O = (0, 1, 0)$, $B = (0, \gamma, 1)$ et $A = -B = (0, -\gamma, 1)$. Rappelons, cf. 3.5.27, que l'opposé de $P = (x, y, z)$ est $-P = (x, -y, z)$. La tangente à Γ en le point de coordonnées (x, y, z) est donnée par les dérivées partielles de l'équation de Γ . C'est la droite $uX + vY + wZ = 0$ avec $u = 6\gamma x^2 - 2\alpha\gamma xz - 2\beta\gamma z^2$, $v = 2yz$ et $w = y^2 - \alpha\gamma x^2 - 4\beta\gamma xz - 3\gamma^2 z^2$. La tangente en B est donc la droite d'équation $Y = \beta X + \gamma Z$. On coupe Γ par cette tangente. On trouve le point B double ($X^2 = 0$) et un point $C = (\alpha\gamma - \beta^2, \alpha\beta\gamma + 2\gamma^2 - \beta^3, 2\gamma)$. On sait qu'alors on a $B \oplus B = -C = (\alpha\gamma - \beta^2, -\alpha\beta\gamma - 2\gamma^2 + \beta^3, 2\gamma)$.

Dire que B est d'ordre 3 signifie qu'on a $B \oplus B = -B = A$. C'est bien équivalent à $\alpha\gamma - \beta^2 = 0$.

Dire que B est d'ordre 4 signifie qu'on a $B \oplus B = -(B \oplus B)$, donc $C = -C$ et c'est bien équivalent à $\alpha\beta\gamma - \beta^3 + 2\gamma^2 = 0$.

4.5.5 Les formules de Cayley

On pourrait utiliser la même méthode pour trouver les conditions d'existence de lignes de Poncelet de période 5, 6, etc. mais les calculs deviennent rapidement inextricables²². Il est plus simple de donner un critère général²³. Nous allons utiliser pour cela les outils de la géométrie algébrique et travailler sur \mathbf{C} pour plus de commodité. Le lecteur est renvoyé à [PG78] pour plus de précisions²⁴.

On reprend la courbe Γ d'équation :

$$Y^2Z + \gamma(2X^3 - \alpha X^2Z - 2\beta XZ^2 - \gamma Z^3) = 0,$$

²²Voir cependant, avec un autre paramétrage de la situation, [Hul07].

²³Pas de vain espoir : la mise en œuvre de ce critère produit aussi des calculs compliqués !

²⁴Ce calcul est dû à Cayley qui aborde plusieurs fois le théorème de Poncelet, la première dans un article de 1853 dans *Philosophical Magazine*, vol. VI, p.99 (Oeuvres, vol. 2, numéro 115). Il voit le polynôme P comme $\det(C - 2\lambda\Omega)$, cf. 4.5.12. Le résultat annoncé est incorrect (sans doute induit en erreur par les cas $n = 3$ et $n = 4$, Cayley affirme, avec les notations ci-dessous, que la condition pour l'existence d'un polygone de Poncelet à n côtés est $a_{n-1} = 0$). Le résultat est corrigé dans le même numéro de revue p. 376 (*loc. cit.* numéro 116). Il n'y a pas de démonstration mais une preuve détaillée se trouve dans un article de 1861 (*loc. cit.* vol. 4, numéro 267).

on en considère les points $O = (0, 1, 0)$ et $B = (0, \gamma, 1)$ et il s'agit de savoir si B est un point d'ordre n de Γ . En termes de diviseurs, cela signifie que le diviseur $nB - nO$ est équivalent à 0, autrement dit, qu'il existe une fonction rationnelle sur Γ qui admet un pôle d'ordre n en O et un zéro d'ordre n en B .

On s'intéresse donc aux fonctions rationnelles admettant un pôle en O . Les fonctions X et Z sont nulles en O et l'équation montre qu'au voisinage de O , Z s'écrit sous la forme uX^3 avec u inversible, de sorte qu'on peut prendre X comme paramètre. Les fonctions rationnelles $x = X/Z$ et $y = Y/Z$ admettent alors un pôle d'ordre 2 (resp. 3) en O et vérifient la relation : $y^2 + \gamma(2x^3 - \alpha x^2 - 2\beta x - \gamma) = 0$ soit $y^2 = -\gamma P(x) := Q(x)$. Au voisinage de $B = (0, \gamma, 1)$, on peut utiliser x comme variable, écrire $y = \sqrt{Q(x)}$ et développer y en série en fonction de x (c'est essentiellement le développement de $(1+x)^{1/2}$) :

$$y = a_0 + a_1x + \dots + a_kx^k + \dots$$

On trouve $a_0 = \gamma$, $a_1 = \beta$, $a_2 = \frac{\alpha\gamma - \beta^2}{2\gamma}$, $a_3 = \frac{1}{2\gamma^2}(\beta^3 - \alpha\beta\gamma - 2\gamma^2)$, $a_4 = \frac{1}{8\gamma^3}(-\alpha^2\gamma^2 + 8\beta\gamma^2 + 6\alpha\beta^2\gamma - 5\beta^4)$, etc.

On considère l'espace vectoriel $H^0(nO)$ des fonctions rationnelles sur Γ admettant un pôle d'ordre $\leq n$ en O . Le théorème de Riemann-Roch indique que cet espace est de dimension n et les fonctions précédentes en fournissent une base. Précisément, si n est impair, $n = 2m + 1$, les fonctions $1, x, \dots, x^m; y, xy, \dots, x^{m-1}y$ en constituent une base, si n est pair, $n = 2m$, ce sont les fonctions $1, x, \dots, x^m; y, xy, \dots, x^{m-2}y$. Notons f_1, \dots, f_n ces fonctions.

Dire que B est d'ordre n c'est dire qu'il existe des scalaires $\lambda_1, \dots, \lambda_n$ non tous nuls tels que la fonction $f = \lambda_1 f_1 + \dots + \lambda_n f_n$ (qui a un pôle d'ordre $\leq n$ en O) admette un zéro d'ordre n en B c'est-à-dire qu'on ait $f(B) = f'(B) = \dots = f^{(n-1)}(B) = 0$ (on dérive ici par rapport à x). L'existence de ces scalaires est donc équivalente à la nullité du déterminant suivant :

$$D_n = \begin{vmatrix} f_1(B) & \dots & f_n(B) \\ f_1'(B) & \dots & f_n'(B) \\ \vdots & \vdots & \vdots \\ f_1^{(n-1)}(B) & \dots & f_n^{(n-1)}(B) \end{vmatrix}.$$

Notons déjà qu'on calcule les valeurs des dérivées en $B = (0, \gamma, 1)$, ce qui revient à faire $x = 0$ dans les fonctions considérées.

Traisons le cas $n = 2m + 1$. Le déterminant se présente sous la forme $D = \begin{vmatrix} A & B \\ 0 & C \end{vmatrix}$ où les $m + 1$ premières colonnes correspondent aux dérivées

des puissances de x . En effet, les dérivées d'ordres $i = 0, 1, \dots, m$ donnent le déterminant diagonal de taille $m + 1$:

$$A = \begin{vmatrix} 1 & 0 & \dots & 0 & 0 \\ 0 & 1! & 0 & \dots & 0 \\ 0 & 0 & 2! & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & m! \end{vmatrix}$$

et les dérivées d'ordre $i > m$ sont nulles. À un scalaire non nul près, le déterminant est donc égal à $\det C$. Le terme général d'indice (i, j) de ce déterminant vaut $\frac{d^{m+i}(x^{j-1}y)}{dx^{m+i}} = (m+i)!a_{m+i-j+1}$ avec $1 \leq i, j \leq m$. En définitive, en mettant en facteur les factorielles et en renversant l'ordre des termes, on trouve, à un scalaire non nul près :

$$D_n = \begin{vmatrix} a_2 & a_3 & \dots & a_{m+1} \\ a_3 & a_4 & \dots & a_{m+2} \\ \vdots & \vdots & & \vdots \\ a_{m+1} & a_{m+2} & \dots & a_{2m} \end{vmatrix}.$$

De la même manière, on obtient, dans le cas $n = 2m$:

$$D_n = \begin{vmatrix} a_3 & a_4 & \dots & a_{m+1} \\ a_4 & a_5 & \dots & a_{m+2} \\ \vdots & \vdots & & \vdots \\ a_{m+1} & a_{m+2} & \dots & a_{2m-1} \end{vmatrix}.$$

On a donc obtenu le critère de Cayley :

4.5.26 Proposition. *Avec les notations précédentes, il existe une ligne de Poncelet de période n si et seulement si le déterminant D_n est nul.*

Pour $n = 3$ le déterminant est simplement a_2 et il est nul si et seulement si on a $\alpha\gamma - \beta^2 = 0$, pour $n = 4$ c'est a_3 , qui est nul si $\beta^3 - \alpha\beta\gamma - 2\gamma^2 = 0$. On retrouve bien les résultats obtenus ci-dessus. Pour $n = 5$, la condition est $a_2a_4 = a_3^2$, soit encore :

$$\beta^6 + 3\alpha^2\beta^2\gamma^2 - 16\gamma^4 - 3\alpha\beta^4\gamma + 8\beta^3\gamma^2 - 8\alpha\beta\gamma^3 - \alpha^3\gamma^3 = 0.$$

4.5.6 Construire des exemples

Dans la pratique, il n'est pas si facile de construire (de manière exacte) des exemples de couples de coniques admettant des lignes de Poncelet périodiques. Nous présentons ici plusieurs manières²⁵, mais chacune est assez vite limitée. Notons que, dans tous les cas, si l'on a produit un tel couple de coniques, on peut le transformer par une homographie (par exemple une homologie) afin d'avoir des coniques de n'importe quel type affine.

La première manière consiste à utiliser les résultats de 4.5.25 pour fabriquer des couples. Pour la période 3 on peut utiliser les paraboles $x = y^2$ (pour Ω) et $y = x^2/2$ (pour C), pour la période 4 la parabole $y = x^2/2$ et l'hyperbole $x = \frac{y^2}{2(1-y)}$.

Une seconde manière s'applique pour $n \leq 5$. Elle consiste à partir d'une conique Ω quelconque et d'un polygone à n côtés inscrit dans Ω , puis à construire C tangente aux côtés de ce polygone et à $5-n$ droites supplémentaires quelconques (ou passant par $5-n$ points arbitraires), voir 4.1.3 et les exercices 4.6.1, 4.6.2, 4.6.4.

Enfin, une troisième façon de faire consiste à partir de deux cercles concentriques et d'un polygone régulier à n côtés inscrit dans l'un et circonscrit à l'autre.

L'intérêt de cette dernière méthode est qu'on est capable de fabriquer des exemples avec n quelconque²⁶. Son désavantage est que les deux coniques sont toujours disjointes²⁷ tandis que les autres méthodes en produisent avec plusieurs points d'intersection.

4.6 Exercices

4.6.1 Constructions

Les exercices suivants sont tous bâtis sur le même mode. On suppose qu'on sait construire une conique donnée par cinq de ces points. C'est le cas par exemple avec le logiciel Cabri géomètre. On se propose de donner des constructions d'une conique à partir de cinq autres éléments, par exemple

²⁵Les figures sont disséminées dans la suite du texte.

²⁶Pas trop grand tout de même !

²⁷Sur \mathbf{R} , car sur \mathbf{C} elles sont bitangentes en des points imaginaires, ce qui montre qu'elles ne rentrent pas tout à fait dans notre cadre théorique puisqu'elles ne sont pas transverses. En effet, un cercle passe par les points cycliques $(1, \pm i, 0)$ et les tangentes en ces points passent par le centre du cercle. Deux cercles concentriques sont donc bitangents aux points cycliques et leurs images par homographie sont des coniques bitangentes.

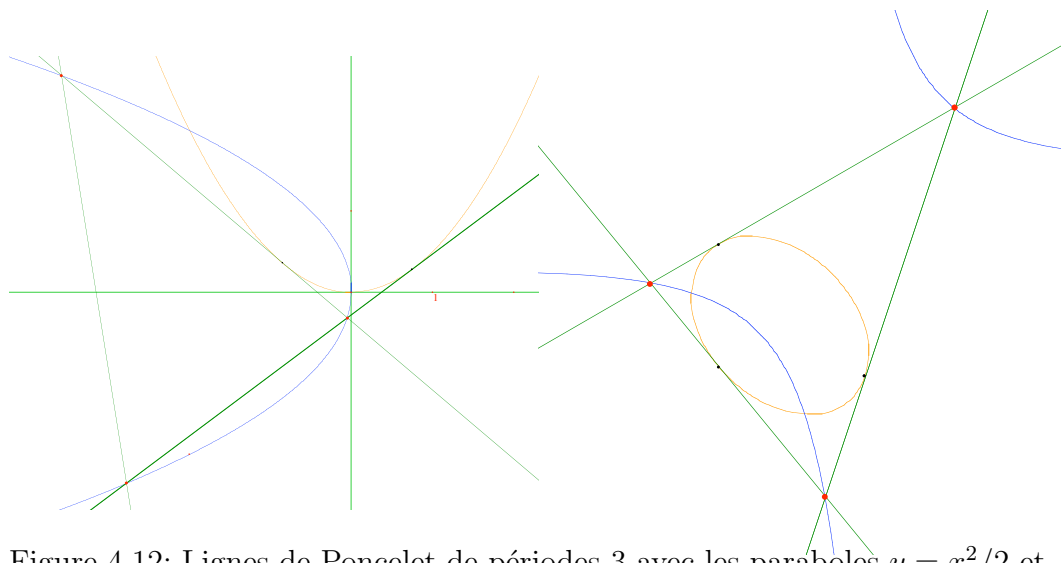


Figure 4.12: Lignes de Poncelet de périodes 3 avec les paraboles $y = x^2/2$ et $x = -y^2/2$, puis avec une hyperbole et une ellipse obtenues par homologie

quatre points et une tangente, etc.

4.6.1 Exercice. Dans cet exercice on construit une conique à partir de quatre points et de la tangente en l'un de ces points. Étant donnés trois points alignés distincts a, b, c , on suppose qu'on sait construire le conjugué harmonique de c par rapport à a, b , voir Partie I, ??.

On se donne quatre points distincts a, b, c, d formant un repère et une droite A passant par a et par aucun des autres points.

a) Montrer qu'il existe une unique conique C passant par a, b, c, d et tangente à A en a et que cette conique est propre.

b) Soit p le point d'intersection de A et (bc) . Construire le conjugué harmonique m de p par rapport à b, c . Soit q le point d'intersection de (am) et de (pd) et e le conjugué harmonique de d par rapport à p, q . Montrer que e est sur C et en déduire une construction de C .

4.6.2 Exercice. Dans cet exercice, on construit une conique Γ à partir de quatre points et d'une tangente (en un point autre que les quatre donnés).

On se donne quatre points distincts a, b, c, d formant un repère et une droite D ne passant par aucun de ces points.

a) Montrer qu'il y a 0, 1 ou 2 coniques Γ passant par a, b, c, d et tangentes à D . (On prendra $a = (1, 0, 0)$, $b = (0, 1, 0)$, $c = (0, 0, 1)$, $d = (1, 1, 1)$ et $D = V(\alpha X + \beta Y + \gamma T)$ et on utilisera 2.2.21.)

b) Construire les points de contact de Γ et D , puis la ou les coniques Γ . (On considère le pinceau des coniques passant par a, b, c, d . Les points

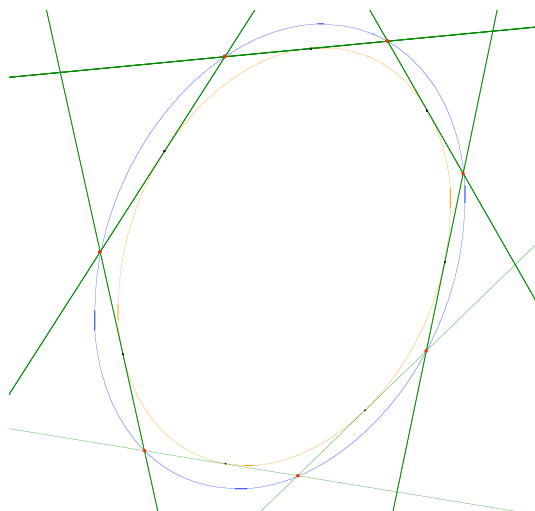


Figure 4.13: Une ligne de Poncelet de période 7

cherchés sont les points fixes de l'involution de Desargues de D associée à ce pinceau (voir 4.4.1) et on les construit à l'aide de 3.6.7.)

4.6.3 Exercice. Cette fois on construit une conique à partir de 3 points et 2 tangentes (en deux de ces points). Soient a, b, c trois points non alignés, A, B deux droites passant respectivement par a et b , mais pas par c , et distinctes de (ab) .

1) Montrer qu'il existe une unique conique C passant par a, b, c et tangente à A, B en a et b et que cette conique est propre.

2) Soit p le point d'intersection de A et B et q le point d'intersection de (pc) et (ab) . Soit d le conjugué harmonique de c par rapport à p, q . Montrer que d est sur C et construire C en utilisant 4.6.1.

4.6.4 Exercice. On considère trois points a, b, c non alignés et deux droites L, M ne passant pas par ces points. Combien y a-t-il de coniques passant par a, b, c et tangentes à L, M ?

4.6.5 Exercice. ¶ L'exercice suivant, qui reprend et prolonge les précédents, utilise des résultats plus avancés de géométrie algébrique. On suppose le corps k algébriquement clos.

1) Montrer que l'ensemble des coniques tangentes à une droite donnée est une hypersurface algébrique de $\mathbf{P}(Q)$, de degré 2 (utiliser 2.2.21 et noter

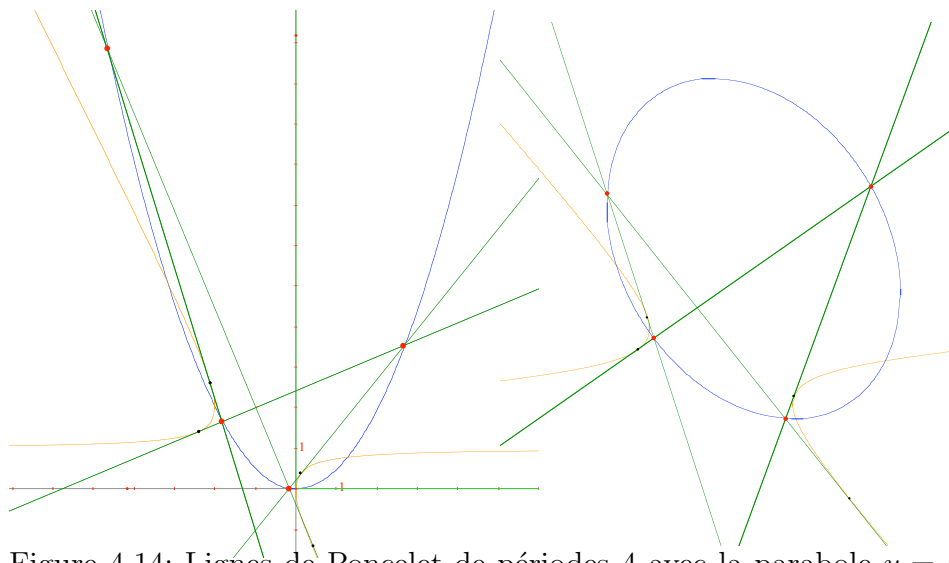


Figure 4.14: Lignes de Poncelet de périodes 4 avec la parabole $y = x^2/2$ et l'hyperbole $x = \frac{y^2}{2(1-y)}$ puis avec une ellipse et une hyperbole obtenues par homologie

que les coefficients de la matrice des cofacteurs d'une matrice A sont des polynômes homogènes de degré 2 en les coefficients de A).

2) En utilisant 1) et le fait que les coniques passant par un point forment un hyperplan de $\mathbf{P}(Q)$, retrouver les résultats de 4.6.2 et 4.6.4 (on utilisera un théorème de Bézout généralisé qui affirme que l'intersection de n hypersurfaces de \mathbf{P}^n , de degrés d_1, \dots, d_n , si elle est finie, est formée de $d_1 \cdots d_n$ points comptés avec des multiplicités).

3) Expliquer pourquoi il y a une unique conique propre tangente à cinq droites en position générale (contrairement à ce que pourrait faire penser une application imprudente²⁸ de Bézout qui en donnerait 32). (Voir 4.1.3.)

4.6.2 Bézout et pinceaux

²⁸La raison est la présence des coniques dégénérées en des droites doubles qui sont tangentes à toutes les droites : l'intersection n'est donc pas finie et le calcul n'a plus aucun sens. On touche là à une partie importante de la géométrie algébrique : la théorie de l'intersection. L'une des questions qui est à l'origine du développement du domaine porte d'ailleurs sur les coniques : combien y a-t-il de coniques tangentes à cinq coniques données. Comme l'hypersurface des coniques tangentes à une conique est de degré 6, Plücker avait donné le chiffre de $6^5 = 7776$ en faisant la même erreur que celle évoquée ci-dessus, avant que Chasles ne rectifie en donnant la bonne valeur : 3264. Voir [WF77] ou [Kle80].

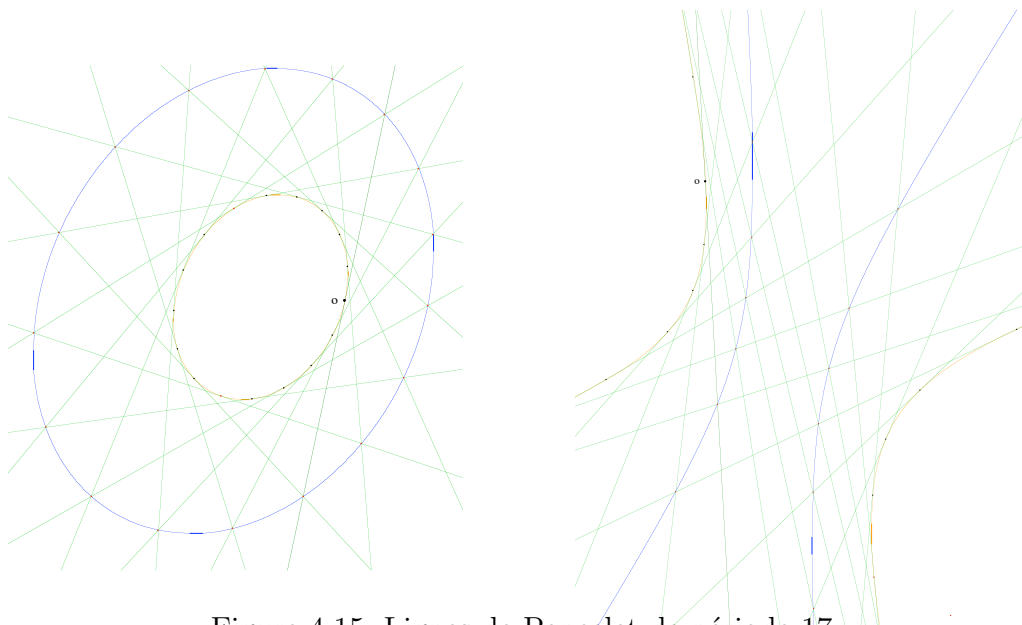


Figure 4.15: Lignes de Poncelet de période 17

4.6.6 Exercice. Cet exercice utilise la notion de résultant pour laquelle on renvoie à [Lan69] Ch. IV, §8. Il s’agit de montrer le théorème de Bézout “faible” 3.5.14.

1) Soit k un corps, P et Q deux polynômes en X et Y de degrés respectifs m et n . Soit $R \in k[X]$ le résultant de P et Q , vus comme polynômes en Y à coefficients dans $k[X]$. Montrer que le degré de R est $\leq mn$. (Utiliser le développement du résultant écrit comme déterminant.)

2) Montrer que, si les polynômes P et Q sont premiers entre eux, l’ensemble $V(P) \cap V(Q)$ des points $(x, y) \in k^2$ qui annulent P et Q est fini. (On montrera qu’il y a au plus mn abscisses et mn ordonnées possibles, donc au plus m^2n^2 points dans l’intersection. On rappelle que le résultant vérifie une “égalité de Bézout” : $R(X) = F(X, Y)P(X, Y) + G(X, Y)Q(X, Y)$.)

3) On suppose désormais k infini et on suppose encore les polynômes P et Q premiers entre eux.

a) Montrer qu’un choix judicieux des axes de coordonnées permet de supposer que deux points de $V(P) \cap V(Q)$ ne sont pas situés sur une même parallèle à l’axe des y . En déduire que le cardinal de $V(P) \cap V(Q)$ est $\leq mn$.

b) Montrer le théorème de Bézout projectif 3.5.14 (on montrera d’abord que l’intersection des deux courbes est finie en distinguant entre points à distance finie et à l’infini ; on changera ensuite de droite à l’infini de façon à éviter les points d’intersection et on appliquera le résultat précédent).

4.6.7 Exercice. On suppose ici $k = \mathbf{R}$ mais on plonge $\mathbf{P}(E) \simeq \mathbf{P}^2(\mathbf{R})$ dans $\mathbf{P}^2(\mathbf{C})$. On se propose d'étudier les pinceaux dont le diviseur d'intersection est incomplet. Soit \mathcal{P} un pinceau non dégénéré. On rappelle que \mathcal{P} contient au plus trois coniques dégénérées.

1) Montrer que \mathcal{P} contient deux coniques propres non vides distinctes. (Prendre deux coniques d'équations q et q' avec $V(q) = \emptyset$. La fonction $m \mapsto -q'(m)/q(m)$ est une fonction continue de $\mathbf{P}(E)$ dans \mathbf{R} . Son image est un intervalle I non réduit à un point. Presque toutes les coniques $\lambda q + q'$ pour $\lambda \in I$ conviennent.)

Dans tout ce qui suit on considère deux coniques propres non vides Γ et Γ' de \mathcal{P} , d'équations q et q' . On suppose que le diviseur $\Gamma \cap \Gamma'$ est de degré < 4 .

2) Montrer que \mathcal{P} contient au moins une conique dégénérée (réelle).

3) On appelle $\bar{\Gamma}$ et $\bar{\Gamma}'$ les coniques complexes d'équations q et q' . Montrer que les seules possibilités pour le diviseur complexe $\bar{\Gamma} \cap \bar{\Gamma}'$ sont les suivantes : quatre points distincts deux à deux complexes conjugués, deux points complexes conjugués chacun de multiplicité 2, deux points réels, éventuellement confondus, et deux points complexes conjugués. Montrer que, dans tous ces cas, le pinceau \mathcal{P} contient une unique conique dégénérée réelle que l'on précisera.

4.6.3 Le groupe de deux coniques

4.6.8 Exercice. Soient Ω et C deux coniques propres transverses, a, b, c, d leurs points d'intersection. On se propose de calculer le groupe $G = G(\Omega, C) := \{f \in PGL(E) \mid f(\Omega) = \Omega \text{ et } f(C) = C\}$.

1) Montrer que G opère fidèlement sur l'ensemble $\{a, b, c, d\}$ et en déduire que G est fini et s'injecte dans \mathfrak{S}_4 . On l'identifie désormais à un sous-groupe de \mathfrak{S}_4 .

2) Montrer que G opère sur les coniques du pinceau \mathcal{P} défini par Ω et C (ou par a, b, c, d) et qu'il permute les trois coniques dégénérées du pinceau. Montrer que le noyau de cette opération est le groupe de Klein V_4 formé de l'identité et des doubles transpositions $(ab)(cd)$, $(ac)(bd)$ et $(ad)(bc)$. En déduire que G contient toujours V_4 .

3) Montrer que G ne contient aucune transposition ni aucun cycle d'ordre 4 (regarder l'action de G sur \mathcal{P}).

4) On suppose que G contient un 3-cycle. Montrer qu'alors le birapport $\llbracket a, b, c, d \rrbracket$ sur l'une ou l'autre conique est égal à $-j$ ou $-j^2$.

5) Montrer que G est égal à V_4 ou \mathfrak{A}_4 selon la valeur de l'invariant défini en 4.2.15. (On pourra par exemple choisir a, b, c, d comme repère et expliciter le groupe G .)

4.6.4 Théorème de Poncelet

Cercles inscrit et circonscrit à un triangle euclidien

4.6.9 Exercice. Le but de cet exercice est de montrer le premier exemple de ligne de Poncelet : le cas d'un triangle du plan affine euclidien et de ses cercles circonscrit et inscrit (ou exinscrits). Le lecteur fera appel à ses souvenirs ou ira se replonger dans les vieux grimoires.

Soit abc un triangle, o le centre du cercle circonscrit Ω à abc (intersection des médiatrices de abc). On note R le rayon de Ω .

Soit i un point du plan, situé sur la bissectrice intérieure de l'angle \widehat{a} du triangle et intérieur au cercle Ω . La bissectrice recoupe Ω en e . On considère le cercle C , de centre i , tangent aux droites (ab) et (ac) . On note r le rayon de C et d la distance oi .

1) Montrer les formules $\sin \frac{\widehat{a}}{2} = \frac{r}{ai} = \frac{be}{2R}$.

2) Montrer les égalités d'angles $\widehat{ebi} = \frac{\widehat{a}}{2} + \widehat{cbi}$ et $\widehat{bie} = \frac{\widehat{a}}{2} + \widehat{iba}$. En déduire que i est sur la bissectrice de \widehat{b} si et seulement si le triangle ebi est isocèle en e , donc si l'on a $be = ie$.

3) Montrer que i est le centre du cercle inscrit au triangle abc si et seulement si on a la formule²⁹ de Chapple (1746) : $R^2 - d^2 = 2rR$ (interpréter $R^2 - d^2$ comme la puissance, au signe près, du point i par rapport à Ω : $ia \cdot ie$, par exemple en utilisant le produit scalaire).

4) On suppose que C est le cercle inscrit à abc . Soit a' un point de Ω . Les tangentes à C issues de a' recoupent Ω en b' et c' . Montrer que $(b'c')$ est tangente à C (c'est le théorème de Poncelet dans ce cas). (Considérer le point i' centre du cercle inscrit à $a'b'c'$ et utiliser 3)).

5) Faire le même travail avec le cercle circonscrit et les trois cercles exinscrits dans les angles a, b, c (on rappelle que les cercles exinscrits sont tangents aux côtés du triangle, leurs centres étant les intersections d'une bissectrice intérieure et de deux bissectrices extérieures).

²⁹Cette formule est parfois attribuée à Euler. Il semble bien que ce soit à tort, voir [HB87], on ne prête qu'aux riches !

Compléments

4.6.10 Exercice. Le but de cet exercice est de prouver que l'application bijective $\pi : W \rightarrow \Gamma_0$ est un isomorphisme au sens des variétés algébriques. Il suffit pour cela de montrer que π et π^{-1} sont définies par des applications polynomiales sur des ouverts affines recouvrant W et Γ_0 .

1) On rappelle que π est donnée par $\pi(X, Y, Z, T) = (X, Y, Z)$ en dehors du point A . On considère le morphisme π' , défini sur l'ouvert $T \neq 0$ de W et à valeurs dans \mathbf{P}^2 , donné par la formule³⁰ :

$$\pi'(X, Y, Z, T) = (YT, -2\beta YT - (\beta^2 - \alpha\gamma)YZ - 2\gamma T^2 - 2\gamma XY, T^2).$$

Montrer que π et π' coïncident sur l'ouvert $ZT \neq 0$ et qu'on a $\pi'(A) = (0, -2\gamma, 1)$ (on multipliera les images de (X, Y, Z, T) par π et π' par T^2 et Z respectivement). En déduire que π est un morphisme de W sur Γ_0 .

2) Montrer que π^{-1} est un morphisme (sur l'ouvert où X et YZ ne sont pas tous deux nuls on utilisera le morphisme donné par (X^2, XY, XZ, YZ) , sur l'ouvert $Y + 2\beta X + 2\gamma Z \neq 0$, on écrira $T = \frac{(\alpha\gamma - \beta^2)XZ - 2\gamma X^2}{Y + 2\beta X + 2\gamma Z}$).

4.6.11 Exercice. Cet exercice a pour but de faire explicitement les calculs de 4.5.24.

1) Soit $a \in \Omega$ un point de paramètres (λ, μ) , D une tangente à C passant par a , de paramètres (ξ, η) . On rappelle que D a pour équation :

$$2\gamma\xi^2x + (\eta^2 + 2\beta\xi\eta + (\beta^2 - \alpha\gamma)\xi^2)y + 2\gamma\xi\eta t = 0.$$

Cette tangente recoupe Ω en a' , de paramètres (λ', μ') . En écrivant que (λ, μ) et (λ', μ') sont les deux racines (homogènes) de l'équation :

$$2\gamma\xi^2\lambda^2 + (\eta^2 + 2\beta\xi\eta + (\beta^2 - \alpha\gamma)\xi^2)\lambda\mu + 2\gamma\xi\eta\mu^2 = 0,$$

montrer qu'on a $\lambda' = \mu\eta$ et $\mu' = \lambda\xi$.

2) Soit D' la deuxième tangente à C passant par a' . On appelle (ξ', η') les paramètres de D' . En écrivant que (ξ, η) et (ξ', η') sont les deux solutions (homogènes) de l'équation en (ξ, η) :

$$2\gamma\xi^2\lambda'^2 + (\eta'^2 + 2\beta\xi'\eta' + (\beta^2 - \alpha\gamma)\xi'^2)\lambda'\mu' + 2\gamma\xi'\eta'\mu'^2 = 0,$$

montrer qu'on a $\xi' = \mu'\eta$ et $\eta' = (2\gamma\lambda' + (\beta^2 - \alpha\gamma)\mu')\xi$.

³⁰La recette qui permet de trouver cette formule est de remplacer (X, Y, Z) par $(X/Z, Y/Z, Z/Z)$ qui va être défini en A car Z s'annule en ce point avec une multiplicité moindre que X et Y .

4.6.12 Exercice. On se propose de calculer $B \oplus B$ dans W .

1) Montrer que la tangente en B est la droite d'équations $2\gamma T + (\beta^2 - \alpha\gamma)X = Y = 0$. En déduire que le plan (B, B, A) tangent à W en B et passant par A est le plan $Y = 0$. Montrer que le quatrième point d'intersection de W avec ce plan est le point $C = B \vee B = (\alpha\gamma - \beta^2, 0, 2\gamma, 0)$.

2) Montrer que le plan (O, A, C) a pour équation $(\beta^2 - \alpha\gamma)Z + 2\gamma X = 0$ et que le quatrième point d'intersection de ce plan avec W est $C' = B \oplus B$:

$$C' = ((\alpha\gamma - \beta^2)^2, -2(\alpha\gamma - \beta^2)(\alpha\beta\gamma - \beta^3 + 2\gamma^2), 2\gamma(\alpha\gamma - \beta^2), -4\gamma(\alpha\beta\gamma - \beta^3 + 2\gamma^2)).$$

(On peut aussi faire ce calcul sur Γ et utiliser π^{-1} pour revenir à W .)

Les cas non transverses

On étudie les cas non transverses par des méthodes analogues à celles employées ci-dessus. On en conserve les notations F, F_1, F_2, V, W , etc.

4.6.13 Exercice. Le cas tangent

On suppose le corps k algébriquement clos. Soient Ω et C deux coniques propres distinctes et tangentes (mais ni bitangentes ni osculatrices).

1) Montrer qu'on peut choisir le repère de telle sorte que Ω et C aient respectivement pour équations $y^2 - xt = 0$ et $y^2 - xt + \alpha y(t - y)$ avec $\alpha \neq 0, 1$. (On choisira le repère de telle sorte que Ω et C soient tangentes en $a = (1, 0, 0)$ et se coupent en $c = (0, 0, 1)$ et $d = (1, 1, 1)$.) On paramètre Ω comme d'habitude par $(\lambda^2, \lambda\mu, \mu^2)$.

2) Montrer que la conique duale C^* admet pour équation $(\alpha u + v)^2 - 4(1 - \alpha)uw = 0$ et qu'elle admet le paramétrage $u = 4(1 - \alpha)\eta^2, v = -4(1 - \alpha)\xi\eta$ et $w = (\xi - \alpha\eta)^2$.

3) On plonge la variété d'incidence V dans \mathbf{P}^3 par le morphisme de Segre. Montrer que l'image est la courbe W d'équations $XT - YZ = 0$ et $4(1 - \alpha)Y^2 - 4(1 - \alpha)XT + (Z - \alpha T)^2 = 0$. Montrer que le point $A = (1, 0, 0, 0)$ est un point singulier de W dont le plan des tangentes est le plan $T = 0$.

4) On projette W à partir du point A sur le plan $X = 0$. Montrer que l'image de W est la conique Γ d'équation $4(1 - \alpha)Y^2 - 4(1 - \alpha)YZ + (Z - \alpha T)^2 = 0$ privée des deux points A_1, A_2 de coordonnées $(1, 2(1 - \alpha \pm \sqrt{\alpha(\alpha - 1)}), 0)$.

On rappelle qu'on a sur $\Gamma - \{A_1, A_2\}$ une loi de groupe (isomorphe à celle de k^*, \times) d'élément neutre $\omega = (0, \alpha, 1)$, voir 3.6.14.

5) On pose $O = (0, 0, \alpha, 1)$. Montrer qu'on a sur W une loi de groupe isomorphe à la précédente, d'élément neutre O , définie de la manière suivante :

pour $P, Q \in W$ on considère le plan (P, Q, A) , il coupe le plan des tangentes en A selon une droite D . On considère le plan défini par D et O , il recoupe W en $P \oplus Q$.

Montrer que l'opposé du point $M = (\alpha^2, \alpha, \alpha, 1)$ est le point $B = (5\alpha^2 - 4\alpha^3, \alpha, 5\alpha - 4\alpha^2, 1)$.

6) Montrer que l'application F est donnée par $F(P) = P \oplus B$. (Si on pose $P' = F_1(P)$ et $P'' = F_2(P')$, on montrera successivement $P \oplus P' = M$, puis $P' \oplus P'' = O$.)

En déduire que le théorème de Poncelet vaut encore dans ce cas.

¶7) Montrer que le point B est d'ordre $n \geq 3$ (et donc que les lignes de Poncelet sont de période n) si et seulement si $r = 1 - 2\alpha + 2\sqrt{\alpha(\alpha - 1)}$ est une racine n -ième de l'unité. (Travailler sur Γ et montrer que r est le birapport $\llbracket A_1, A_2, \omega, B' \rrbracket$ où B' est l'image de B dans Γ .)

Montrer qu'on a un triangle de Poncelet (resp. un quadrilatère) si et seulement si on a $\alpha = 3/4$ (resp. $\alpha = 1/2$).

4.6.14 Exercice. Le cas bitangent

Soient Ω et C deux coniques bitangentes en a et c .

1) Montrer qu'on peut supposer que les coniques Ω et C ont respectivement pour équations $y^2 - xt = 0$ et $y^2 - 2\alpha xt = 0$ (on choisira le repère de telle sorte que les contacts soient $a = (1, 0, 0)$ et $c = (0, 0, 1)$). En déduire que C^* a pour équation $\alpha v^2 - 2uw = 0$.

2) Montrer que les coniques Ω et C^* admettent les paramétrages $(\lambda^2, \lambda\mu, \mu^2)$ et $(\alpha\xi^2, 2\xi\eta, 2\eta^2)$ et que l'équation d'incidence³¹ est :

$$\alpha\lambda^2\xi^2 + 2\lambda\mu\xi\eta + 2\mu^2\eta^2 = 0.$$

3) Montrer que si une ligne de Poncelet contient a ou c elle ne contient que ces points et leurs tangentes. On supposera désormais que les lignes ne passent pas par ces points. On peut alors supposer qu'on a $\mu = \eta = 1$ et repérer les points (resp. les tangentes) par le seul paramètre $\lambda \neq 0$ (resp. $\xi \neq 0$).

4) On note r_1, r_2 les racines de l'équation $\alpha r^2 + 2r + 2 = 0$. Montrer que le couple (λ, ξ) correspond à un point de la variété d'incidence si et seulement si $\lambda\xi$ est égal à r_1 ou r_2 . Soit (λ, ξ) un couple vérifiant $\lambda\xi = r_1$. Montrer que l'application de Poncelet lui associe le couple (λ', ξ') avec $\lambda' = \frac{r_2}{r_1}\lambda$ et

³¹Il est inutile dans ce cas de plonger la variété d'incidence dans \mathbf{P}^3 . Si on le fait on voit que l'image W est la réunion de deux coniques propres non coplanaires se coupant en deux points.

$\xi' = \frac{r_1}{r_2}\xi$. En déduire que la ligne polygonale issue d'un point est périodique de période n si et seulement si r_1/r_2 est une racine n -ième de l'unité et en déduire le théorème de Poncelet.

Montrer qu'on a un triangle de Poncelet (resp. un quadrilatère) si et seulement si on a $\alpha = 2$ (resp. $\alpha = 1$).

5) On suppose α réel. Montrer qu'on a un polygone de Poncelet d'ordre n si et seulement si α est égal à $\frac{1}{1 + \cos \frac{2k\pi}{n}}$. (Cas particulier, $n = 5$, $\alpha = 3 - \sqrt{5}$.)

6) Traiter directement le cas des cercles concentriques (qui sont des coniques bitangentes en les points cycliques). (On montrera que, si le cercle Ω est de rayon 1 et le cercle C de rayon r , on a $\alpha = 1/(2r^2)$).

4.6.15 Exercice. Le cas osculateur

Soient Ω et C deux coniques osculatrices en a et sécantes en c .

1) Montrer qu'on peut supposer que les coniques Ω et C ont respectivement pour équations $y^2 - xt = 0$ et $y^2 - xt + \alpha yt = 0$ avec $\alpha \neq 0$. En déduire que C^* a pour équation $\alpha^2 u^2 + 2\alpha uv - 4uw + v^2 = 0$

2) Montrer que les coniques Ω et C^* admettent les paramétrages $(\lambda^2, \lambda\mu, \mu^2)$ et $(4\eta^2, 4\xi\eta, (\xi + \alpha\eta)^2)$. On plonge la variété d'incidence dans \mathbf{P}^3 par le plongement de Segre. Montrer qu'on obtient la courbe W d'équations $XT - YZ = 0$ et $4Y^2 + 4YZ + Z^2 + \alpha^2 T^2 + 2\alpha ZT = 0$.

3) Montrer que la courbe W admet l'unique point singulier³² $S = (1, 0, 0, 0)$ et que la projection de centre ce point sur le plan $X = 0$ induit un isomorphisme de $W - \{S\}$ sur la conique Γ d'équation $4Y^2 + 4YZ + Z^2 + \alpha^2 T^2 + 2\alpha ZT = 0$ privée du point $E = (1, -2, 0)$.

4) On considère la loi de groupe abélien sur $\Gamma - \{E\}$, d'origine $O = (0, -\alpha, 1)$, définie comme en 3.6.15. On rappelle que ce groupe est isomorphe au groupe additif $(k, +)$.

a) Montrer que l'application de Poncelet F_2 , vue sur Γ , est l'application $P \mapsto -P$ (on montrera que P et $F_2(P)$ sont alignés avec le point $\omega = (0, 1, 0)$, intersection des tangentes à Γ en O et E).

b) On pose $A = (\alpha, -\alpha, 1)$. Montrer que l'application F_1 est l'application $A \mapsto A - P$.

c) En déduire que l'application F est donnée par $F(P) = P \oplus B$ avec $B = -A = (\alpha, -5\alpha, 1)$ et montrer le théorème de Poncelet.

³²On notera que ce point correspond au cas où le drapeau de départ est formé du point et de la tangente d'osculation, donc est stationnaire.

d) Montrer que, dans le cas osculateur, il n'existe pas de lignes de Poncelet de période $n \geq 3$, sauf dans le cas où la caractéristique du corps divise n .

4.6.16 Exercice. Le cas surosculateur

Soient Ω et C deux coniques surosculatrices en a .

1) Montrer qu'on peut supposer que les coniques Ω et C ont respectivement pour équations $y^2 - xt = 0$ et $y^2 - xt + \alpha t^2 = 0$ avec $\alpha \neq 0$. En déduire que C^* a pour équation $4\alpha u^2 + 4uw - v^2 = 0$.

2) Montrer que les coniques Ω et C^* admettent les paramétrages $(\lambda^2, \lambda\mu, \mu^2)$ et $(4\eta^2, 4\xi\eta, \xi^2 - 4\alpha\eta^2)$. Montrer qu'on peut supposer (en dehors du cas évident où l'on part du point a ou de sa tangente) que les coniques sont paramétrées par $\lambda, \xi \in k$.

3) En écrivant la relation d'incidence, montrer qu'on a $F(\lambda, \xi) = (\lambda - 2\sqrt{\alpha}, \xi + 4\sqrt{\alpha})$. En déduire l'expression de F^n et le théorème de Poncelet et montrer qu'il n'y a pas de lignes de Poncelet de période $n \geq 3$, sauf dans le cas où la caractéristique du corps divise n .

La preuve de Poncelet

Les exercices suivants sont inspirés de la preuve proposée par Poncelet lui-même.

4.6.17 Exercice. Le cas des triangles

On reprend les notations usuelles Ω et C ainsi que les équations et paramétrages vus en 4.5.11. Soient $p = (\lambda^2, \lambda\mu, \mu^2)$ et $m = (a^2, ab, b^2)$ deux points de Ω .

1) Vérifier que la droite (pm) a pour équation $\mu bX - (\lambda b + \mu a)Y + \lambda aT = 0$. (Dans le cas où les points sont égaux on vérifiera qu'on obtient la tangente à Ω en p .)

2) Montrer que la droite (pm) est tangente à C si et seulement si le paramètre (a, b) de m est solution de l'équation : $ua^2 + vab + wb^2 = 0$ avec $u = -\lambda^2$, $v = -2(\beta\lambda\mu + \gamma\mu^2)$ et $w = (\alpha\gamma - \beta^2)\mu^2 - 2\gamma\lambda\mu$. Montrer qu'il y a deux³³ solutions m_1, m_2 à cette équation et que la droite (m_1m_2) est la droite d'équation $uX + vY + wT = 0$.

3) On suppose que le point p varie sur Ω et que les points m_1, m_2 sont les points d'intersection de Ω et des tangentes à C issues de p . Montrer que la droite (m_1m_2) enveloppe une conique Γ . Calculer une équation de Γ^* en

³³On précisera le cas où elles sont confondues.

éliminant λ, μ entre u, v, w (on écrira la relation $(\lambda\mu)^2 = \lambda^2\mu^2$), puis calculer une équation de Γ .

On note encore Ω, C, Γ les matrices définissant ces coniques. Montrer la formule $\Gamma = (\beta^2 - \alpha\gamma)\Omega + \gamma C$ et en déduire que Γ est dans le pinceau (Ω, C) .

4) Montrer le théorème de Poncelet pour $n = 3$ (si on a un triangle de Poncelet pour Ω et C , on montrera qu'on a $\Gamma = C$). Retrouver le critère numérique assurant cette condition.

4.6.18 Exercice. Le cas général

On reprend encore les notations usuelles. Soient $p = m_0, m_1, \dots, m_r$ des points de Ω . On suppose qu'il existe des coniques C_1, \dots, C_r appartenant au pinceau (Ω, C) , telles que, pour $i = 1, \dots, r$, $(m_{i-1}m_i)$ soit tangente à C_i . Il s'agit de montrer que la droite (m_0m_r) enveloppe une conique du pinceau.

1) Montrer que ce résultat implique le théorème de Poncelet pour les polygones à r côtés.

2) ¶¶¶ Montrer³⁴ le résultat pour $r = 2$.

3) Conclure en raisonnant par récurrence sur r .

4.6.19 Exercice. Cet exercice a pour objectif de discuter la méthode de Poncelet et notamment le principe de continuité. Dans sa preuve, Poncelet se ramène au cas de deux cercles par projection, en étant bien conscient que ces cercles peuvent être imaginaires. L'exercice a pour but de montrer que cet état de fait est incontournable.

On travaille dans le plan affine euclidien, plongé dans $\mathbf{P}^2(\mathbf{R})$ (la droite $T = 0$ est choisie comme droite à l'infini) et on plonge le tout dans $\mathbf{P}^2(\mathbf{C})$. Les cercles passent tous par les points cycliques $I = (1, i, 0)$ et $J = (1, -i, 0)$.

1) Soit C le cercle réel d'équation projective $X^2 + Y^2 - T^2 = 0$ et soient M, M' deux points de C dans le plan projectif complexe. Montrer que si les points M, M' sont réels (resp. imaginaires conjugués) le birapport $\llbracket I, J, M, M' \rrbracket$ est un complexe de module 1 (resp. un réel). (On paramétrera le cercle par $x = u^2 - v^2, y = 2uv, t = u^2 + v^2$.)

2) Soient Ω et C deux coniques propres de $\mathbf{P}^2(\mathbf{C})$ et a, b, c, d leurs points d'intersection supposés distincts. Montrer que l'invariant double birapport $(\llbracket a, b, c, d \rrbracket_\Omega, \llbracket a, b, c, d \rrbracket_C)$ (voir 4.2.13) peut prendre toutes les valeurs dans $(\mathbf{C} - \{0, 1\})^2$. En déduire qu'il n'existe pas, en général, d'homographie de $PGL(3, \mathbf{C})$ transformant deux coniques transverses en deux cercles réels.

³⁴Le lecteur qui parviendrait à prouver ce résultat tout seul et sans autre indication eût été sans nul doute un autre Poncelet s'il n'était né trop tard, dans un siècle trop vieux. Pour les autres on conseille la lecture de [HB87].

Bibliographie

- [Arc60] Archimède. *Oeuvres complètes, traduction P. Ver Eecke*. A. Blanchard, Paris, 1960.
- [Art62] Emil Artin. *Algèbre géométrique*. Gauthier-Villars, Paris, 1962.
- [Ber90] Marcel Berger. *Géométrie*. Nathan, Paris, 1990.
- [CP74] Lucien Szpiro Christian Peskine. Liaison des variétés algébriques. *Invent. Maths.*, 26 : 271–302, 1974.
- [Die70] Jean Dieudonné. *La géométrie des groupes classiques*. Springer, Berlin, 1970.
- [DP90] Mireille Martin-Deschamps Daniel Perrin. Sur la classification des courbes gauches. *Astérisque*, 184-185 :1–207, 1990.
- [Ful69] William Fulton. *Algebraic curves*. Benjamin, New-York, 1969.
- [Ful84] William Fulton. *Intersection Theory*. Springer Verlag, Berlin, 1984.
- [Har77] Robin Hartshorne. *Algebraic geometry*. Springer, Berlin, 1977.
- [HB87] F. Oort D.W. Raven H.J.M. Bos, C. Kers. Poncelet’s closure theorem. *Expo. Math.*, 5 :289–364, 1987.
- [Hul07] Dominique Hulin. Factorisation des polynômes de poncelet. *Geom. Dedicata*, 130 :109–136, 2007.
- [Hus87] Dale Husemöller. *Elliptic Curves*. Springer Verlag, Berlin, 1987.
- [Kle80] S.L. Kleiman. Chasles’s enumerative theory of conics : a historical introduction. *Math. Assoc. Amer. Stud. Math.*, 20 :117–138, 1980.
- [Lan69] Serge Lang. *Algebra*. Addison Wesley, New-York, 1969.
- [Per95] Daniel Perrin. *Géométrie algébrique, une introduction*. Interéditions, Paris, 1995.
- [Per96] Daniel Perrin. *Cours d’algèbre*. Ellipses, Paris, 1996.
- [Per05] Daniel Perrin. *Mathématiques d’École*. Cassini, Paris, 2005.
- [PG78] Joseph Harris Phillip Griffiths. On cayley explicit solution to poncelet’s porism. *J. enseign. Math.*, II série, 24 :31–40, 1978.

- [RD89a] Daniel Caire Robert Deltheil. *Compléments de géométrie*. Jacques Gabay, Paris, 1989.
- [RD89b] Daniel Caire Robert Deltheil. *Géométrie*. Jacques Gabay, Paris, 1989.
- [Sil86] J. Silverman. *The Arithmetic of Elliptic Curves*. Springer Verlag, Berlin, 1986.
- [WF77] R. MacPherson W. Fulton. *Defining algebraic intersections, in Algebraic Geometry, Proceedings Tromsø1977*. Springer Verlag, Lecture notes in Math. 687, Berlin, 1977.